Agence des services frontaliers du Canada | Canada Border Services Agency

Access to Information and Privacy (ATIP) Division Handbook

PROTECTION • SERVICE • INTÉGRITÉ

Canada

TABLE OF CONTENTS

DEFINITIONS 9
USEFUL REFERENCES 13
1. INTRODUCTION 15
- **1.1** Purpose of the ATIP Division Handbook 15
- **1.2** How to Read the ATIP Division Handbook 15
- **1.3** Access to Information and Privacy Division 15

2. TYPES OF ATIP REQUESTS RECEIVED 17
- **2.1** Travel History Requests 17
- **2.2** Privacy Act Requests 17
- **2.3** Access to Information Act Requests 18
- **2.4** Access Consultations 18
- **2.5** Internal Vettings 18
- **2.6** Informal Requests 18

3. WHO CAN MAKE A REQUEST? 19
4. PRINCIPLES FOR ASSISTING APPLICANTS 20
ADMINISTRATION SECTION 21
5. RECEIVING AND OPENING NEW REQUESTS 22
- **5.1** Receiving Requests 22
  - *5.1.1 Regular Mail or Fax Requests* 22
  - *5.1.2 Email Requests* 22
  - *5.1.3 On-line Requests* 22
- **5.2** Searching for a Cross-Reference in APCM 23
  - *Cross-Reference* 23
  - *NOTEtoFile* 26
- **5.3** Entering a New Client in APCM 26
- **5.4** Adding Request Information in APCM 27
  - *InitialSetUp* 31
- **5.5** Adding Payment Information for Access to Information Requests 32
  - *Payment Received* 32
- **5.6** Refunding Payment Information for Access to Information Requests 34
  - *Payment Returned* 34

6. ADDING DOCUMENTS IN REDACTION 36
- **6.1** Changing Printer Properties for Redaction 37
  - *DocType (A)* 40

7. MAILING OUT AND FINAL QUALITY CHECK 42
- **7.1** Regular Mail-outs 42
  - *Mailed Out* 43
- **7.2** Burning a CD 43

7.3 Final Quality Check 51
Quality Control 51
7.4 Courier Mail-outs (Speedy) 52
8. RETURNED MAILED 55
Returned Mail 55
PRODUCTION UNIT SECTION 57
9. TRANSFERRING AN ATIA REQUEST TO ANOTHER GOVERNMENT INSTITUTION 57
10. ASSIGNMENT OF A FILE TO AN ANALYST 58
AssignReview 58
SPECIAL INSTRUCTIONS 59
AssignReview 59
11. SEARCHING FOR CROSS REFERENCES 60
Cross-Reference 60
12. ACKNOWLEDGEMENT INCOMPLETES (IF REQUIRED) 62
ACKincomplete 62
12.1 When the Missing Information Is Received 63
12.2 Closing an Abandoned File 64
13. PROCESSING THE DIFFERENT TYPES OF REQUESTS 67
13.1 Travel History Requests 68
13.1.1 *Using GCMS for TH Requests* 68
13.1.2 *Running a TH report* 72
SYSTEM NOTES (e): 76
13.1.3 *Exit Reports in COGNOS* 78
13.1.4 *Reviewing Travel History Records* 86
REVIEW 86
13.1.5 *Responding to a Travel History Request* 92
RESPONSE Traveller History 92
13.1.6 *Exporting your Travel History Reports* 97
EXPORT/PRINT 97
13.2 Privacy and Access to Information Requests (not True Access) 100
13.2.1 *GCMS or FOSS Notes* 100
SYSTEM NOTES 100
13.2.2 *Immigration Records* 104
13.2.2.1 NCMS 104
13.2.2.2 Adding your System Notes in APCM 106
SYSTEM NOTES 106
RETRIEVALnotice 109
REVIEW 109
RESPONSE 110
RESPONSEadditionalinfo 110
13.2.3 *Grievance or HR Files* 110

RETRIEVALnotice 110
REVIEW 111
RESPONSE 111
13.2.4 Any and all Emails held by the Following People about Me 111
RETRIEVALnotice 111
13.2.4.1 Accessing Emails of Absent Employees 112
REVIEW 113
RESPONSE 113
RESPONSEadditionalinfo 113
13.3 Access to Information Requests (True Access) 113
RETRIEVALnotice 114
13.3.1 Recording Recommendations of the OPI 114
13.3.2 Reviewing True Access Files 117
REVIEW 117
13.3.3 Agree / Disagree / Resolving Recommendations 117
MANDATORY > Recommendations – AGREE with 118
MANDATORY > Recommendations – DISAGREE with 118
MANDATORY > Recommendations – RESOLVED with 118
13.3.4 Response Letter 119
RESPONSE 119
RESPONSEadditionalinfo 119
13.3.5 Flags 119
HEADS-UP Formal (+): LEGAL (Director Approval) 119
HEADS-UP Formal to (+): 119
HEADS-UP Informal to: 119
13.3.6 Uploading onto the Public Safety Portal (True Access Only) 121
13.4 Email In-box Requests (True Access) 121
RETRIEVALnotice 121
13.4.1 Retrieving Emails from the Z: Drive 124
13.4.2 Exporting Emails to Excel and to Redaction 125
13.4.3 Notification of the Individual 130
13.4.4 Phase 1 - Review 132
REVIEW 132
13.4.5 Response Letter – Phase 1 132
RESPONSEphase1 132
13.4.6 Phase 2 - Review 133
13.4.7 Recording Recommendations of the OPI 133
13.4.1 Agree / Disagree/ Resolving Recommendations 134
13.4.2 Response Letter – Phase 2 134
RESPONSE 134
13.4.3 Flags 134
HEADS-UP Formal (+): LEGAL (Director Approval) 134
HEADS-UP Formal to (+): 134

HEADS-UP Informal to: 134
13.4.4 *Uploading onto the Public Safety Portal (True Access Only)* 134
13.5 Access Consultations (ACs) or Privacy Consultations (PCs) 134
13.5.1 *Due Date* 135
13.5.2 *RESPONSE LETTER* 135
RESPONSE Consult 135
13.5.3 *SECRET Records* 138
13.6 Internal Vettings 138
13.6.1 *Acknowledgement of Receipt and Due Date* 139
ACKaccept 139
13.6.2 *Review* 143
REVIEW 143
Communicated with 143
13.6.3 *Response Letter – Privacy or Access Vetting* 144
RESPONSEPrivacyVetting 144
14. SENDING RETRIEVALS 149
14.1 Clarification after Tasking 152
Communicated with: 152
14.2 No Response to your Retrieval? 154
Follow-up 154
15. PRINTING TO REDACTION, STACKS AND INDEXING 157
DocType (A): 160
16. REVIEWING RECORDS 162
16.1 Recording Recommendations of the OPI 162
16.1.1 *Highlighting in Redaction* 162
16.1.2 *Custom Stamps* 162
16.2 Recording Notes in Redaction 164
16.3 Triaging Records 165
16.4 Extensions 165
16.5 Exemptions and Exclusions 165
16.5.1 *Exemptions* 165
16.5.2 *Exclusions* 166
16.6 Reviewing your Records 167
16.6.1 *Redacting Information* 167
16.6.2 *Paginating your Records* 169
16.6.3 *Closing Screen* 169
17. APPLYING EXTENSIONS 173
EXTENDvolume 174
EXTENDConsultation 175
EXTEND3rd Party 175
17.1 Adding the Extension in APCM 175

17.3 Standard Extension Times for Certain OGDs ... 179

18. SENDING CONSULTATIONS ... 182

18.1 Internal Review ... 182

CONSULTops ... 182

CONSULTindividual ... 182

Legal Advice Sought ... 182

OPIReleaseCopy ... 182

18.2 OGD Consultations ... 182

CONSULTfederalDept ... 182

18.3 Cabinet Confidences ... 182

CONSULT – CABINETConfidence ... 182

18.3.1 Consultation with DLSU on the applicability of Cabinet Confidences ... 182

18.3.2 Cabinet Confidences – Section 69 ... 183

CONSULT – CABINETConfidence ... 183

18.4 Other Consultations ... 183

CONSULTprovince/municipality/police ... 183

CONSULT3rdParty ... 184

18.5 Creating a Consultation in APCM ... 184

19. MANAGING SECRET RECORDS ... 191

19.1 Receiving SECRET Records ... 191

DocType (A): ... 191

19.2 Consulting SECRET Records ... 192

19.3 Reviewing SECRET Records ... 193

19.4 Preparing SECRET Records for Approval ... 196

19.5 Approved SECRET Records ... 198

20. RECORDING DELAYS AND LEVEL OF COMPLEXITY ... 202

20.1 Complexity (Access and Privacy files only) ... 202

MANDATORY > COMPLEXITYLegal ... 202

MANDATORY > COMPLEXITYOther ... 203

20.2 DELAY / DEEMED REFUSAL REASONS (Access and Privacy files only) ... 204

MANDATORY > DELAYREASONWorkload ... 204

MANDATORY > DELAYREASONExternalConsult ... 204

MANDATORY > DELAYREASONInternalConsult ... 204

MANDATORY > DELAYREASONOther ... 204

21. PREPARING YOUR RESPONSE LETTER ... 206

21.1 Additional Records Response ... 210

22. APPROVAL OF FILES ... 213

22.1 Approval and Signature Actions ... 213

ApprovalFinal ... 213

Signature ... 213

22.2 Preliminary Approvals ... 216

APPROVALpreliminary 216
22.3 Transferring a File to your Team Leader 217
22.4 True Access Approvals 218
22.4.1 Assistant Director / Director's Reviews 218
Assistant Director's Review 218
Director's Briefing / Review 218
22.4.2 Communications Review 219
HEADS-UP Format to (+): 219
23. SIGNING A LETTER ELECTRONICALLY 224
23.1 Signing a Letter using Adobe 224
23.1 Signing a Letter using Microsoft Word 227
24. EXPORTING YOUR RELEASE PACKAGE 231
EXPORT/PRINT 231
Quality Control 233
25. MAIL-OUT 235
Mailed Out 235
Deleted from Retrieval Folder 237
26. UPLOADING ONTO THE PUBLIC SAFETY PORTAL (TRUE ACCESS) 240
27. RETRIEVING GCMS RECORDS 243
27.1 Logging into GCMS 244
27.2 Searching in GCMS 245
27.3 GCMS Applications 246
27.4 GCMS eDocs 249
27.5 GCMS Correspondence 256
27.6 CAIPS Records 261
27.7 Printing your Records into Redaction 262
28. RETRIEVING FOSS RECORDS 266
29. AUDIO / VIDEO FILES 271
29.1 The Vetting Process of Audio/ Video 273
30. COMPLAINTS 278
30.1 Receiving Complaints 278
30.2 Logging a Complaint into APCM 279
30.3 Recording a Complaint Received Action in APCM 280
COMPLAINTreceived 280
30.4 Recording the Investigator Package Action in APCM 281
Investigator Package 281
OIC_EAW 284
OIC_Form A 284
OIC_Form B 284
30.5 Assigning a Complaint 285

COMPLAINTassignment 285
30.6 Processing a Complaint 286
COMPLAINTCorrespondence 286
LITIGATIONFlag 287
NegotiatedDisclosureDate 287
REPRESENTATIONSec35 287
30.7 Closing a Complaint 287
31. ACCESS TO INFORMATION ACT ARTICLES **289**
32. PRIVACY ACT ARTICLES **295**
33. CRIMINAL OFFENCE UNDER THE ACCESS TO INFORMATION ACT (S. 67.1) **299**
34. PROGRAMS AND INFORMATION HOLDINGS (FORMERLY INFO SOURCE) **300**
34.1 Informal Requests 300
ANNEX A: OPERATIONS TEAM CHECKLIST **301**
ANNEX B: ANALYST AND TEAM LEADER CHECKLIST **302**
ANNEX C: ATIP IMMIGRATION TASKING GRID **305**
ANNEX D: STACKING AND INDEXING **306**
ANNEX E: LETTER INSERTS **309**
ACK/INCOMPLETE LETTERS 309
NO RECORDS LETTERS 312
LATE RESPONSE PARAGRAPH 313
ANNEX F: TIPS AND TRICKS **314**
ANNEX G: RETENTION OF FORMS **316**
ANNEX H: INFORMATION CLASSIFICATION GUIDE **317**

DEFINITIONS

This section provides definitions of terminology relevant to the Access to Information and Privacy Division:

Access to Information and Privacy Annual Reports	Reports submitted by the head of a government institution to Parliament on the administration of the *Access to Information Act* and *Privacy Act* during the financial year.
APCM – Access Pro Case Management	A database program used to track and process all incoming requests in the Access to Information and Privacy Division.
Applicant/ Requester	An individual who makes a formal request to access records under the *Access to Information Act* or the *Privacy Act*.
ATIA – Access to Information Act	A term used to describe the *Access to Information Act* – also used as a general term for an official Access to Information request. Access to Information requests can either be an individual seeking their personal information directly or through a representative, or they are in search of corporate records about the Canada Border Services Agency. Requests seeking non-personal information are known as "True ATI" or "True Access" requests.
ATIP – Access to Information and Privacy	A general term that can be used to describe either a request submitted by a client looking for information, or it may refer to the Access to Information and Privacy office of a government department.
ATIP Coordinator	The official designated for each government institution to coordinate all activities relating to the application of the *Access to Information Act* and the *Privacy Act*, including regulations, directives and guidelines within the institution.
ATIP Shared Drive	A location on the CBSA network established by ATIP to allow documents to be placed on to avoid the need of mailing records to HQ. The drive is set up so each Liaison Officer has their own folder, and within that folder they will set up folders specific to each request number, and place all pertinent documents in that location. The Liaison Officer (LO) only has access to their folder and they cannot access folders from other regions/offices, for security reasons.
Cognos (exits)	A database containing information held by the Canada Border Services Agency. The Access to Information and Privacy Division has limited access to this system and can retrieve Travel History Reports (entries and exits) for a client.
Confidentiality	Information that must not be disclosed to unauthorized individuals, because of the resulting injury to national or other interests, with reference to specific provisions of the *Access to Information Act* and the *Privacy Act*.
Complainant	An applicant who makes a complaint to the Information Commissioner of Canada or the Privacy Commissioner of Canada on the grounds set forth in subsection 30(1) of the *Access to Information Act* and section 29 of the *Privacy Act*.

Delegate	An officer or employee of a government institution who has been delegated by the *Privacy Act Heads of Government Institutions Designation Order* to exercise or perform the powers, duties, and functions of the head of the institution under the *Access to Information Act* and *Privacy Act*.
Disclosure	The release of information by any method (e.g., verbal, provision of a copy, examination of a record) to any person or body.
Excluded information	Information to which the *Access to Information Act* and the *Privacy Act* do not apply, includes published material or material available for purchase to public; library or museum material made, acquired and preserved solely for public reference or exhibition purposes; and private material placed with Library and Archives Canada or in the national museums of Canada; and Confidences of the Queen's Privy Council of Canada.
Exemption	A provision of the *Access to Information Act* and the *Privacy Act* that entitles the head of the institution to refuse to disclose information in part or in its entirety, in response to a request received under the Acts.
Formal Access/ Privacy Request	A request to obtain records under the control of a government institution that is made in writing, with specific reference to either the *Access to Information Act* (ATIA) or the *Privacy Act*. In the case of an ATIA request, a $5 application fee is applied.
FOSS – Field Operations Support System	An obsolete database containing immigration information of clients of the Canada Border Services Agency. The Access to Information and Privacy Division has access to this system and will retrieve information from there without the need of assistance from the regions. This program has been archived and ATIP does still gather information from the FOSS library.
GCMS – Global Case Management System	A database containing information held by Canada Border Services Agency. The Access to Information and Privacy Division has access to this system and will retrieve information from there without the need of assistance from the regions.
Head of Agency	The person responsible for ensuring that its organization complies with the *Access to Information Act* and the *Privacy Act*. In addition, the Minister of the Treasury Board coordinates the administration of the Acts by preparing and distributing policies and guidelines to help institutions interpret the laws and to assist them in applying the laws to high-profile issues.
ICES - The Integrated Customs Enforcement System	A database containing information held by the Canada Border Services Agency. The Access to Information and Privacy Division has limited access to this system and can retrieve Travel History Reports (*entries only*) and Highway Passage reports for a client. Any other information held in the database is provided by the Office of Primary Interest (OPI).
Information Commissioner of Canada/ Privacy Commissioner of Canada	Ombudsmen appointed by Parliament to investigate complaints in respect of any matter relating to requesting or obtaining access to records under the *Access to Information Act* and the *Privacy Act* respectively. In addition, the Privacy Commissioner investigates

complaints regarding the collection, use, disclosure, retention and disposal of personal information.

Info Source — A Treasury Board of Canada Secretariat publication containing details on the organization, programs, functions and information holdings of all federal institutions subject to the Access to Information Act and the Privacy Act.

LO – Liaison Officer — A designated employee [illegible] within the Canada Border Services Agency. The [illegible] areas are as follows: Atlantic Region, Programs Branch, Corporate Affairs Branch, [illegible], Greater Toronto Area Region, Human Resources Branch, Information, Science and Technology Branch, Northern Ontario Region, Operations Branch, Pacific Region, Prairie Region, Quebec Region, [illegible], Southern Ontario Region, Human Resources [illegible], Southern Ontario Region.

NCMS – National Case Management System — A centralized database to track immigration enforcement cases involving [illegible] detentions, hearings, interventions, appeals, investigations and removals. The Access to Information and Privacy [illegible] uses the system for reference purposes, to determine where a file is located, whether or not an investigation is active [illegible], and to help the analyst better understand the information [illegible]. The database is provided by the Office of [illegible] (OPI).

OGD – Other Government Department — Are the government offices, whether a department, agency or federal institution, outside of the Canada Border Services Agency.

OPI – Office of Primary Interest — The branch or program area within a government institution whose functions, work and information holdings are most relevant to the subject matter of a request. The OPI is responsible for the subject matter to which the request relates or holds the personal information requested.

Personal Information — Information about an identifiable individual as defined in section 3 of the Privacy Act. The definition in the Privacy Act is not exhaustive, as indicated by the introductory phrase [illegible] the generality of the foregoing [illegible] mentioned in the list may also be included in the definition of personal information if it qualifies as information about an identifiable individual.

PA – Privacy Act — A term used to describe the Privacy Act. Also used as a general term for an official Privacy request. These requests are clients seeking copies of their personal information held by the Agency.

Privacy Breach — The improper or unauthorized creation, collection, use, disclosure, retention or disposal of personal information.

Privacy Commissioner — An independent Officer of Parliament who oversees government institutions' compliance with the Privacy Act and reports directly to the House of Commons and the Senate.

Record — Any documentary material, regardless of medium or form.

Redaction (AccessPro)	Imaging/redlining software used in conjunction with the Access Pro Case Management
Release Package	The completed documents that are sent to the client at the completion of their Access to Information or Privacy request. Your Access to Information release packages are void of all non-releasable personal and corporate information and the records can be released to anyone seeking them. You can consult the Open Information web page for a synopsis of past true Access to Information requests, which anyone can request, for free, informally. https://open.canada.ca/en/search/ati
SME – Subject Matter Expert	The person within the OPI that provides the documents for the request. They also have the opportunity to provide any recommendations with those documents, as to what should and should not be released to the client. The ATIP Analyst will review the recommendations and determine whether they can or should be applied to the file. Depending on the nature of the file, the SME may be contacted to further justify or explain the reasoning behind their recommendations as it may not fall within the scope of the Acts.
Third Party	Any person, group of persons or organization other than the person that made the request or a government institution. This includes Federal Crown corporations and other government organizations to which the Access to Information Act and the Privacy Act do not apply.
Third-Party Information	Trade secrets, financial, commercial, scientific or technical information supplied to government; information that if disclosed would cause financial loss or prejudice the competitive position of a third party; or information that if disclosed would interfere with contractual or other negotiations.
Under the Control	A record is under the control of a government institution when that institution is authorized to grant or deny access to it, to govern its use and, subject to the approval of the Librarian and Archivist of Canada, to dispose of it. Records in the physical possession of an institution are presumed to be under its control. Records held elsewhere on behalf of an institution are still under its control.

USEFUL REFERENCES

URLs may change without notice. Please report any broken links to CBSA-ASFC_ATIP-AIPRP@cbsa-asfc.gc.ca

Useful Links	
APOM login	
[illegible] Login	
[illegible]	
IRCC Office Codes	
ATIP Coordinator Contacts	http://www.tbs-sct.gc.ca/hgw-cgf/oversight-surveillance/atip-aiprp/coord-eng.asp
IRCC Acronyms	
Access to Information Act Court Cases (OIC)	http://www.oic-ci.gc.ca/eng/court-cases.aspx
Office of the Information Commissioner of Canada (OIC)	http://www.oic-ci.gc.ca/eng/
Office of the Privacy Commissioner of Canada (OPC)	https://www.priv.gc.ca/[illegible]
TBS Policies	
Policy on Privacy Protection	http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12510&section=text
Directive on Privacy Practices	http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=18309
Directive on Privacy Requests and Correction of Information	http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18311&section=text
Policy on Access to Information	http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12453&section=text
Legislation and Regulations	
Privacy Act	http://laws-lois.justice.gc.ca/eng/acts/P-21/
Privacy Regulations	http://laws-lois.justice.gc.ca/eng/regulations/SOR-83-508/index.html
Customs Act	http://laws-lois.justice.gc.ca/eng/acts/[illegible]
Access to Information Act	http://laws-lois.justice.gc.ca/eng/acts/A-1/
CBSA Policies	

Info Source	http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/[illegible]
Policy on the Disclosure of Business Information: Section 107 of the Customs Act	http://atlas/[illegible]
Policy on the Disclosure of Personal Information: Section 8 of the Privacy Act	http://atlas/[illegible]

1. INTRODUCTION

1.1 Purpose of the ATIP Division Handbook

The Access to Information and Privacy (ATIP) Division Handbook is intended to provide guidance and promote consistency in the processing of all Access to Information and Privacy requests within the Canada Border Services Agency (CBSA). The handbook is also a valuable tool to train new employees and those changing responsibilities within the Administration and Production Units.

The ATIP Division Handbook has been developed by the Canada Border Services Agency's (CBSA) Access to Information and Privacy (ATIP) Directorate, ATIP Policy & Governance (AP&G) Unit. The Handbook will remain an evergreen document subject to updates and revisions at the discretion of the Director, ATIP.

1.2 How to Read the ATIP Division Handbook

The ATIP Division Handbook is intended to be read in an electronic format (.pdf) to leverage hyperlinks for quick access to relevant information.

Readers are encouraged to familiarize themselves with entire document as a whole. However, it is not necessary to read the Handbook sequentially. Each section is written for a specific audience to address the individual elements in the processing of different types of requests.

1.3 Access to Information and Privacy Division

The Access to Information and Privacy (ATIP) Division is comprised of five units: an Administration section, three Production units, and two Policy units.

The Administration section's function is to receive all incoming requests and consultations, to ensure quality control of all outgoing correspondence, and to support the Production units in their day-to-day business.

The Production units (ATIP Production units A, B and C) assign all branches and regions with retrieval requests and provide daily operational guidance and support to CBSA employees.

Typically the roles within the three ATIP Production units are as follows:

- Junior Analysts – Process travel history requests, and small immigration files.
- Senior Analysts – Process Access and Privacy requests, complex immigration, verbals, consultations and True Access requests.
- Team Leaders – Approve all requests above, and provide guidance, support and training (when required) to Analysts.

<u>Assistant Directors</u> – Approve True Access requests, and provide guidance and support to Analysts and Team Leaders.

The <u>ATIP Policy and Governance</u> unit develops policies, tools, and procedures to support ATIP requirements within the CBSA and provides training to employees.

The <u>Information Sharing and Collaborative Arrangement Policy</u> unit maintains the policy framework for the CBSA's information-sharing and domestic written collaborative arrangements.

The ATIP Coordinator for the CBSA is the Executive Director of the Information Sharing, Access to Information and Privacy Division. This Division is part of the Corporate Secretariat which reports to the Vice-President of the Strategic Policy Branch. Consistent with <u>best practices</u> identified by the Treasury Board of Canada Secretariat (TBS), the CBSA's ATIP Coordinator is positioned within three levels of the President and has full delegated authority, reporting directly to the Director General of the Corporate Secretariat, who in turn reports to the Vice-President of the Strategic Policy Branch.

Key to maintaining compliance with the statutory time requirements of the *Access to Information Act* and *Privacy Act* is the ATIP Division's ability to obtain records from branches and regions in a timely and reliable manner. Supported by a network of [illegible] ATIP liaison officers across the CBSA, the ATIP Division is well positioned to receive, coordinate, and process requests for information under the Acts.

The ATIP Division works closely with other members of the PS portfolio, including the Canadian Security Intelligence Service, the Correctional Service of Canada, the Parole Board of Canada, and the Royal Canadian Mounted Police, to share best practices and develop streamlined processes for the retrieval of jointly held records within the 30-day legislated time frame required to respond to *Access to Information* requests.

2 TYPES OF ATIP REQUESTS RECEIVED

The *Access to Information Act* and the *Privacy Act* came into effect on July 1, 1983. These Acts provide Canadian citizens, permanent residents or any person (or entity) present in Canada the legal right to obtain information, in any form, that is under the control of a government institution. The general purpose of these acts is to make government more open and transparent, allowing citizens to more fully participate in the democratic process.

The Canada Border Services Agency (CBSA) Access to Information and Privacy (ATIP) Division processes a variety of requests every day, some examples are:

2.1 Travel History Requests

A Travel History Report is a record of a traveller's entries into Canada. The report documents entries made on or after August 1, 2000. This information is collected by the CBSA on all travellers entering Canada.

Traveller exit information is also available in a limited capacity but applies only to foreign nationals leaving Canada at a land port only since June 30th, 2013 (no exit information exists prior to that date). Exit information is also not recorded for Canadian citizens and American citizens.

A Highway Passage Report may also be requested, but this report only indicates that a specific license plate has entered into Canada and does not specify the individual(s) that were in the vehicle.

2.2 Privacy Act Requests

The *Privacy Act* protects the privacy of individuals with respect to personal information about them held by a government institution and provides individuals with a right to access and request corrections to this information.

Section 7 of the *Privacy Act* stipulates that personal information can only be used in accordance with the purpose for which the information was collected or for a use consistent with that purpose. Information protected by the *Privacy Act* can only be disclosed with the consent of the person to whom it relates or in accordance with the exception terms of subsection 8(2) of the *Privacy Act*.

Records, regardless of the format, held under the control of a federal government institution (listed in the Schedule of the Act) are subject to the *Privacy Act*. There are a few exceptions: documents that are published or available for purchase and confidences of the Queen's Privy Council. This information is excluded and, therefore, the Act does not apply to these records.

With respect to all other types of records, certain information may require exemption from access, such as information relating to national defense and security, law enforcement, and personal information concerning other individuals.

2.3 Access to Information Act Requests

The *Access to Information Act* gives individuals a right to access records under the control of a federal government institution. The main principles of this Act are: government information should be available to the public, exemptions to this right should be limited and specific, and decisions on disclosure of information should be reviewed independently of government.

Records, regardless of the format, held under the control of a federal government institution (listed in Schedule I of the Act) are subject to the *Access to Information Act*. There are a few exceptions such as documents that are published or available for purchase or confidences of the Queen's Privy Council. This information is excluded and, therefore, the Act does not apply to these records.

With respect to all other types of records, certain information may require exemption from access, such as information relating to national defense and security, law enforcement, the administration of economic and social programs and other individuals' personal information.

2.4 Access Consultations

As an integral part of departmental processing procedures, other government institutions are consulted if access requests contain issues of interest to them. Formal consultations are undertaken in writing and initiated between ATIP offices as required in order to facilitate the completion of many Access to Information requests.

2.5 Internal Vettings

The ATIP Division provides advice to departmental staff with respect to informal requests, parliamentary questions and the review of draft audit, evaluation, security and harassment reports.

2.6 Informal Requests

A summary list of completed Access to Information requests is published on the Open Government website on a monthly basis. These informal requests are Access to Information requests for previously released Access to Information packages.

3. WHO CAN MAKE A REQUEST?

Privacy Act Right of Access

Any individual present in Canada can make a request under the *Privacy Act*. Canadian citizens and permanent residents also have the right to make a request under the *Privacy Act* from outside Canada. An individual who is not a Canadian citizen or a permanent resident cannot make a request from outside Canada, and such a request cannot be made by a representative who is a Canadian citizen, permanent resident or a person present in Canada on behalf of the individual. A request on behalf of an individual needs to be made under the *Access to Information Act*. There are no fees for requesting information under the *Privacy Act*.

Access to Information Right of Access

Any individual present in Canada can make a request under the *Access to Information Act*. Canadian citizens and permanent residents also have the right to make a request under the *Access to Information Act* from outside Canada. An individual who is not a Canadian citizen or a permanent resident cannot make a request from outside Canada unless it is made by a representative who is a Canadian citizen, a permanent resident or a person present in Canada on behalf of the individual. Requests made pursuant to the *Access to Information Act* must include a $5.00 application fee.

4. PRINCIPLES FOR ASSISTING APPLICANTS

Protect your applicant's identity

Limiting, on a need to know basis, the disclosure of information that could directly or indirectly lead to the identification of a requester, unless the requester consents to the disclosure. And to process a request without regard to the requester's identity.

- **Provide guidance including right to complain**

Offer reasonable assistance throughout the request process. Provide guidance on the Access to Information Act or Privacy Act, including information on the processing of a request and the right to complain to the appropriate Commissioner of Canada.

⇒ **Provide accurate, complete and timely access**

Provide accurate and complete responses. Assist the requester in reformulating the request where it would result in the person receiving more accurate, complete and timely access. Make every reasonable effort to locate and retrieve the requested records or personal information under the control of the government institution. Apply limited and specific exemptions to the requested records or personal information.

Adopt a broad interpretation and provide prompt clarification

Adopt a broad interpretation of a request, but inform as appropriate and without undue delay when the request needs to be clarified. When a request has been clarified or its wording altered, document the wording of the revised request and the date of the revision in the tracking system (APCM).

⇒ **Provide records in the format requested**

When privacy, confidentiality and security considerations would not be compromised and it would not be unreasonable or impracticable to do so, provide records in the format requested by the requester, including machine-readable and reusable formats. Provide an appropriate location within the government institution to examine the requested information, when required.

Offer informal processing when possible

Determining whether it is appropriate to process the request on an informal basis, and offering the requester the possibility of treating the request informally and explaining that only formal requests are subject to the provisions of the Act.

⇒ **Provide contextual information as appropriate**

Providing, as appropriate, general information of a contextual nature in response to an Access request to help the requester understand the record in cases where the record itself may provide misleading information and the Analyst has been informed by the Office of Primary Interest (OPI) that the information contained in the record may be misleading. Note:

Government institutions are not obligated to explain all records or complex information being disclosed when responding to an Access request.

[redacted]

6. RECEIVING AND OPENING NEW REQUESTS

When a client wishes to receive information from a government institution they can either submit their request on-line via the Access to Information and Privacy Online Request website, email their request to the Access to Information and Privacy Division generic mailbox CBSA-ASFC_ATIP-AIPRP@cbsa-asfc.gc.ca, fax or use regular mail. In all instances, the client must provide the government department with enough information to allow the institution to locate the documents in question.

When a request is received the information is then entered into Access Pro Case Management (APCM) and an Access to Information and Privacy (ATIP) file number is created. The file is labelled alphanumerically with an indication of the Act that the request falls under, the year the file is being processed and a sequential number (e.g. A-2017-01234, P-2017-56789).

5.1 Receiving Requests

6.1.1 Regular Mail or Fax Requests

All hardcopy requests received by fax or regular mail are placed in the appropriately labeled bin (sorted by type of request) near the black cabinet. Requests received by fax or priority post are date stamped and take priority over the regular mail. Faxes received after 4:00pm or on weekends are date stamped for the following business day. Regular mail requests are date stamped on the day they are entered in the system.

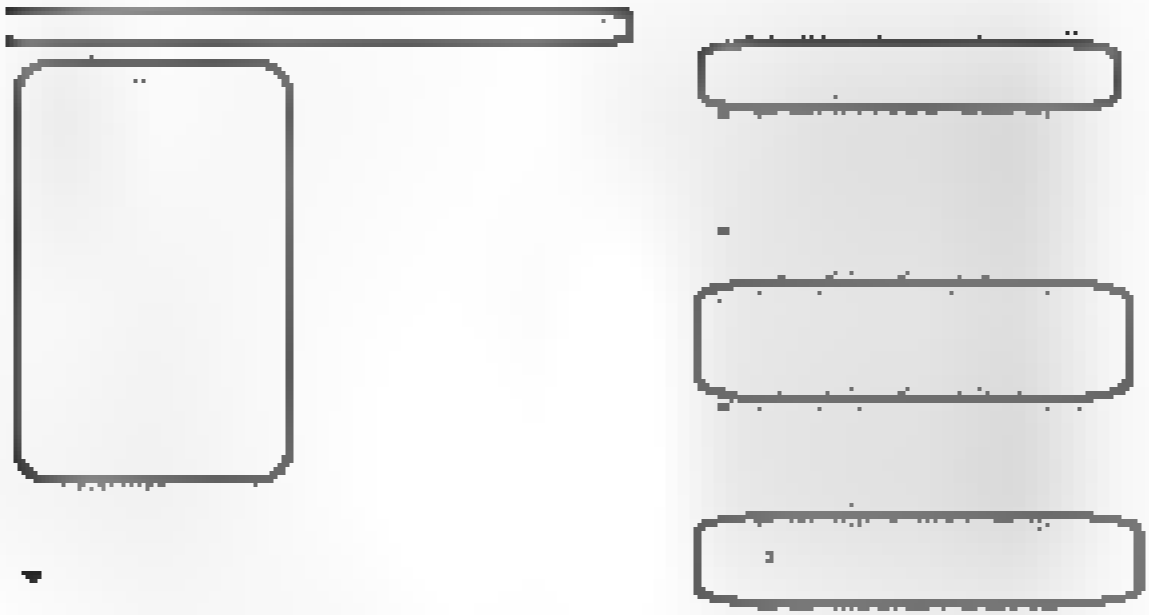
6.1.2 Email Requests

Any email requests received via the Access to Information and Privacy Division generic mailbox CBSA-ASFC_ATIP-AIPRP@cbsa-asfc.gc.ca are stored in a "green box" folder under the generic email inbox. Folders are created using the received date and any emails received after 4:00pm or on weekends are considered received the following business day.

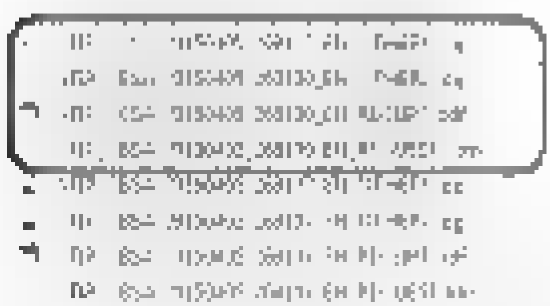
6.1.3 On-line Requests

Any on-line requests via the Access to Information and Privacy Online Request website are placed in the "Inbound OMEGA" shared network drive.

In the drive, select about 20 files and move them into the folder with your name on it. This will ensure that no one else will be opening the same files as you. Make sure that the ones you highlight include all attachments for that specific request (note the numbers on the files).



Look at the files, now located in your folder and find the one that says **REQUEST** and double click on it to read the request. In the below example there are 3 attachments for the request:



When you double click on the **REQUEST** file, a window will then open in Internet Explorer with all details for the request, including the person's personal information and the request text. It is important to verify if this is a duplicate request, before you enter it in the system. Duplicates are easily found by doing a cross-reference search.

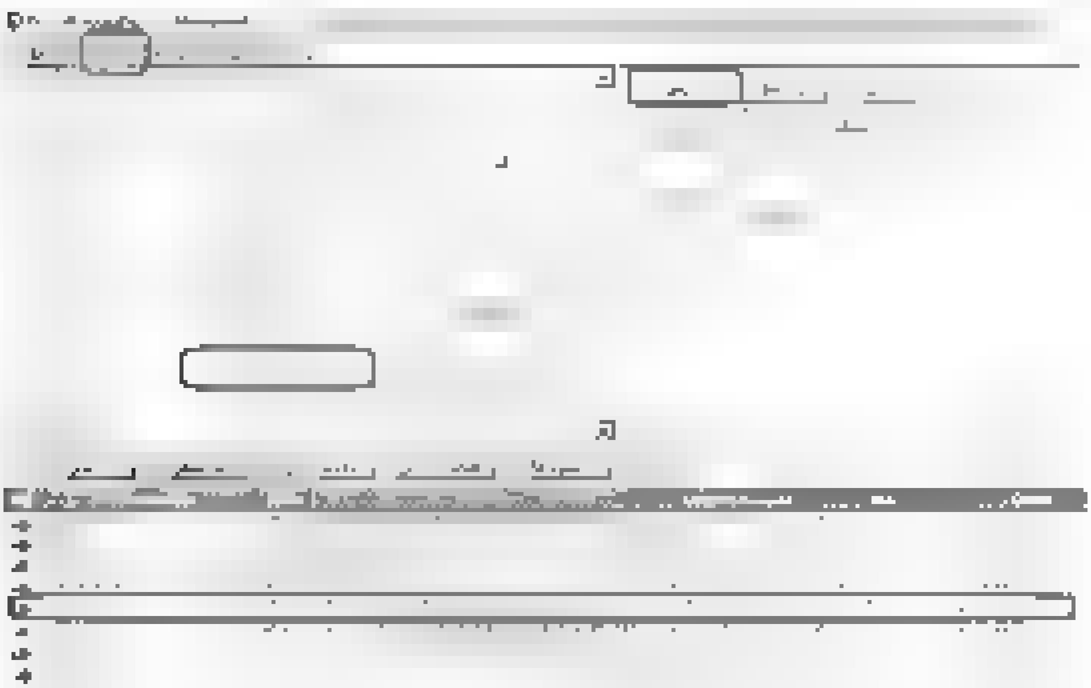
5.2 Searching for a Cross-Reference in APCM

Cross-Reference

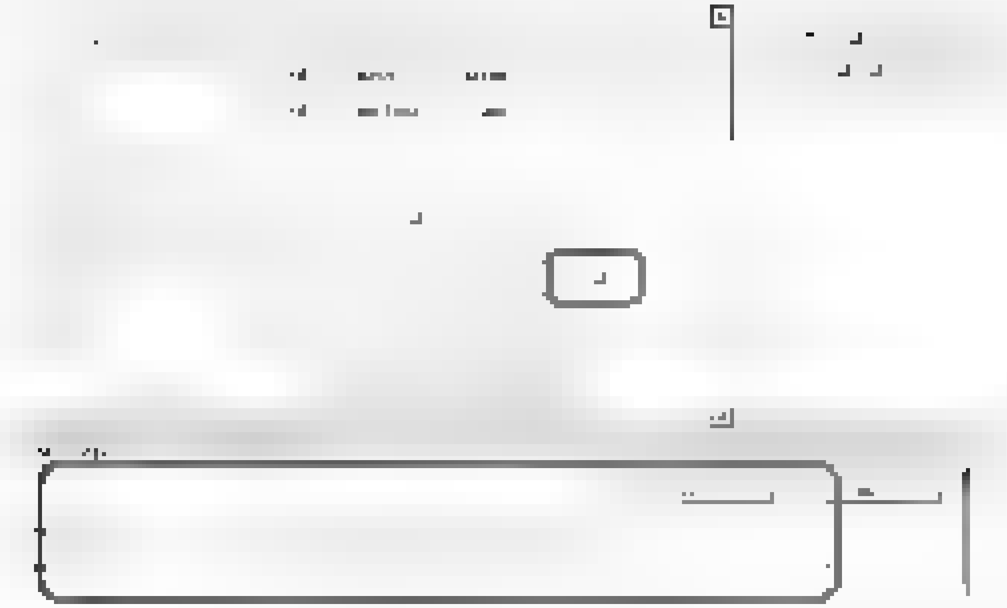
Looking at the request, you will now do a search in APCM to locate any cross-references there may be. Locate any key words in the text (ie. a person's name, or FOSS – CLIENT ID number, or if

If it is not for personal information a key term being used like "Enforcement Manual") and search those words in the "full text" area in APCM

If you find any files that are from the same person about themselves or if the request is asking for the same information (ie. Enforcement Manual) write that number down. For individuals write all the file numbers down. For generic items, use your judgement, but if it is generic like the enforcement manual, just include the most recent file number.



Also do a search for the requester in the Search Requester area

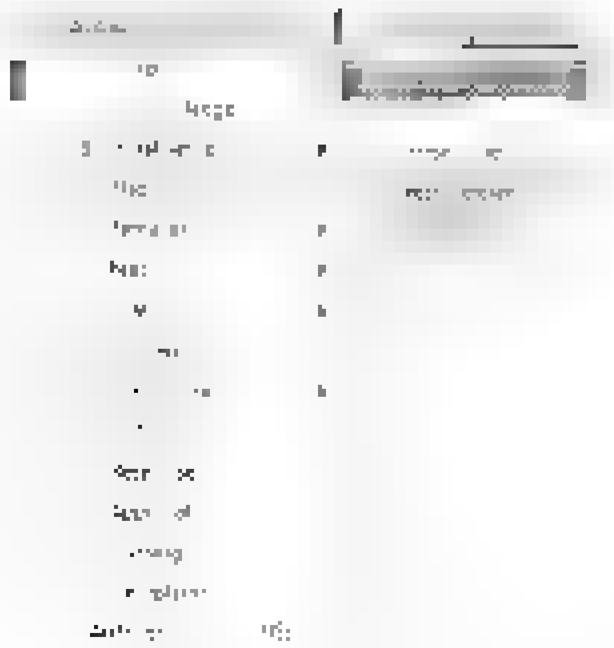


Note: If you find the exact match for the requester there will be no need to add the request again.

Click **Next** at the bottom of screen. Go to the request screen in APCM and click **Add**.

If a cross-reference is found, add the action in APCM, select "B – Initial Set up" then Cross-Reference and note the relevant file number "A-20 -XXXXX/CDO" in the comment box including the initials of the Analyst. Do not add any other information in the comment box, and if there is more than one cross-reference list all.

If there is no cross-reference found, please place the action "Cross-Reference" and nil in the comment field.



NOTEtoFile

If you have additional information to add, use the **NOTEtoFile** action (located in 1-Other).

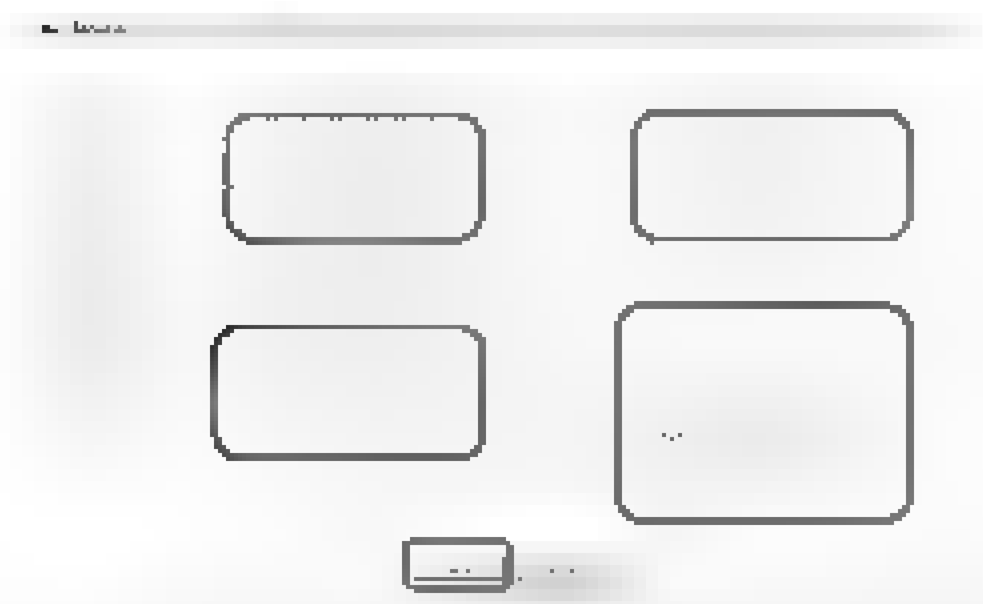
6.3 Entering a New Client in APCM

A new window will appear. If you found the client already in the system, type their name into the fields, and click **Search**. When you find the right name, highlight it and click **Next**.

If the requester's name is not found, click **Add Requester**.

All the information that you need to fill out this screen will be on the "Request form"

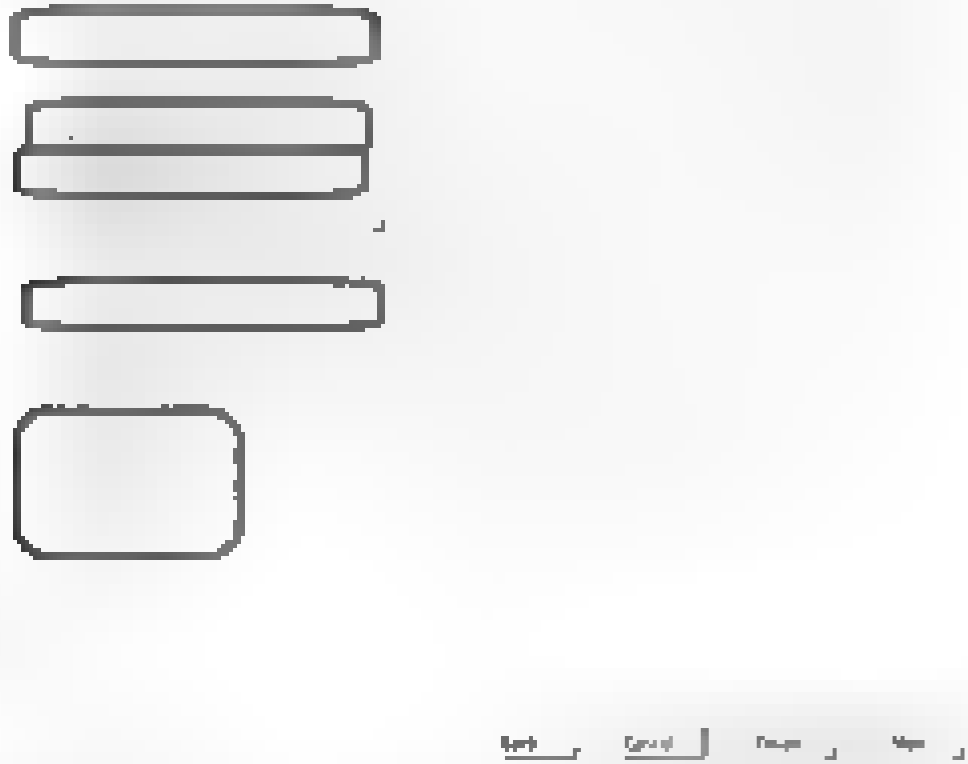
Make sure you fill out the following fields



Everything can be copied and pasted from the request to the appropriate field on the form if this is an online request; if not, you will just have to type it in. If the client entered their information in all CAPS, please do not copy and paste that as this is the information that would go on a letter to the client and it cannot go out with all letters in CAPS. When you are finished with adding the client's information, click Save, a new window will appear.

6.4 Adding Request Information in APCM

Provide information on the following



Pick the Act they are requesting the information from, change the officer to "NEW REQUEST NEW REQUE... If the request is for Travel History, in the Category field, pick "TH" - NEW Requests"

With an online request, the packet number is located on the request and you fill it out as follows: the date tracking number, e.g. 20170403-123456; the date on the request is the submitted date on the request. The Date Initially (DI) received and Date Complete (DC) received will be the submission date, however if it was received after 16:00 (4:00) it will be the following business day. Requests made on weekends, the DI and DC are the next Monday.

For email, fax or mail in there will be no file number (unless they have specified one in their letter head, you can then input that). Both received dates will be the date it was "date stamped" in our office.

Enter the Appropriate Category

1. To be categorized (default) * requesters that do not say what they are looking for*

2. Travel History

- Only travel history information is requested
- Clerks will change categories for travel history files

True Access

- CBSA information in which the release package is suitable for public disclosure (does not contain any confidential personal or customs client information)
- Summary of request posted to Open Data site and included in MO Weekly Reports

4. Immigration Client File
   - Only (or predominantly) immigration client file information

5. Employee File
   - Requester is a CBSA employee asking for emails about themselves
   - Requester is a CBSA employee looking for HR files related to them (grievance, staffing, etc)

6. Other
   - Any other type of request that does not belong in the other categories

Enter the Source (Access and Privacy files)

Media

- Includes journalists, reporters and researchers for newspapers, television or other media

Academia

- Includes professors (university, college, vocational), teachers, educators, students and academic researchers

Business

- Includes representatives of private sector companies or corporations, information brokers, lawyers (unless they are requesting personal information as representative for client), agents, consultants, paid lobbyists, etc

Organization

- Includes associations, unions, not-for-profit and voluntary organizations, offices of Members of Parliament, political parties, non-government organizations, etc.

Public

- Includes individuals and any person not included in the categories identified above

Decline to identify

- For online requests when indicated by the client

CBSA Internal – not for A or P)

- Access and Privacy Settings

Other Can Fed Govt

- Other Canadian federal government institutions

Non-Can Fed Government

- Provincial, municipal, or foreign governments
- Organizations
- Non-governmental organizations

When entering the "full text" please use the following guidelines

Travel History Requests:

For travel history where exits are not specified, always type the following full text

Travel history for {LAST NAME, First Name – DOB December 19, 1958 – Client ID – XXXX-XXXX Passport (if given)}. Period January 1, 2000 to January 1, 2015

For travel history where exits are requested, always type the following full text

Entries and exits for {LAST NAME, First Name – DOB December 19, 1958 – Client ID – XXXX-XXXX – Passport (if given)}. Period: from January 1, 2000 to January 1, 2015

All Other Requests:

For all other requests you can copy and paste what the client has written. If the client is asking for their personal information, make sure that the full text has the first and last name (last name in CAPS), the DOB and if possible the Client ID/FOSS number. For all personal information (name, DOB, Client ID/FOSS, etc.) you will need to make sure that you put that information between privacy brackets { } so the information does not appear in any ATIP reports.

Also, use your best judgement as to what is needed in the full text as people often include information that is not needed, or disclose additional personal information in the body of the text. If the client has provided their SIN number DO NOT include it in the request text and make sure you remove it from the actual request using the tools menu in Adobe Acrobat.

When entering your "summary" text you can highlight the text you have placed in "full text", hold down the control key and then press the letter "c" and release the keys. This action will copy the text. Now click the mouse in the "summary" box and hold down the control key again and then press the letter "v". This will paste the text in the summary box. The summary box can only hold a certain number of characters, so it is possible the entire text won't show. Please find

a finishing point that makes sense, and add "(...)" at the end of the text. Only do this if your full text is too long to paste into the summary box.

An example can be shown here:

Summary

Traveller's API/PNR information - Last airport of departure before arrival in Canada: London; First airport of arrival in Canada: Toronto; Date: November 08, 2017; Time of arrival at Canada: 6:00am; Airline: Delta; Flight number: 12345 (...)

When you are finished entering the "full text" and "summary text" click **Next** and another window will appear.

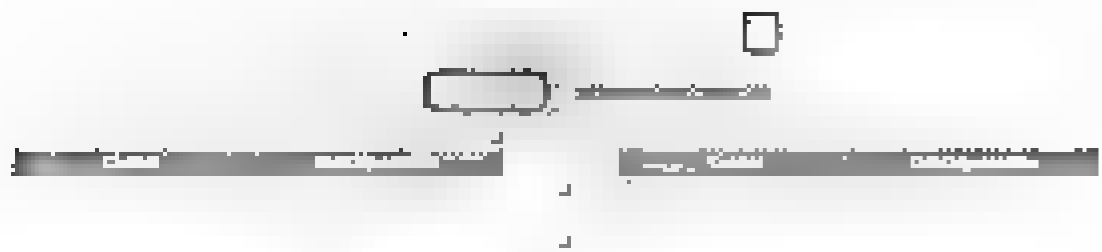
Initial Set-Up

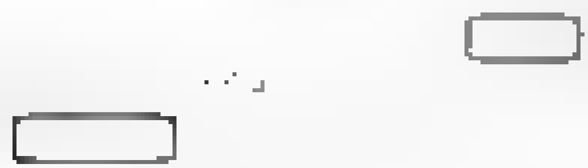
In the Action name, change the action to **Initial Set-Up**, and in the comments section add one of the following:

- online - (your initial)
- fax - (your initial)
- email - (your initial)
- paper - (your initial)

Please DO NOT divert from these 4 options (this is very important for when we pull our reports; if we see variations of them it would affect the accuracy of our results).

Click **Finish** when done. Please refer to the example below.





The request will close, but it will be still highlighted. Double click to open the action screen again.

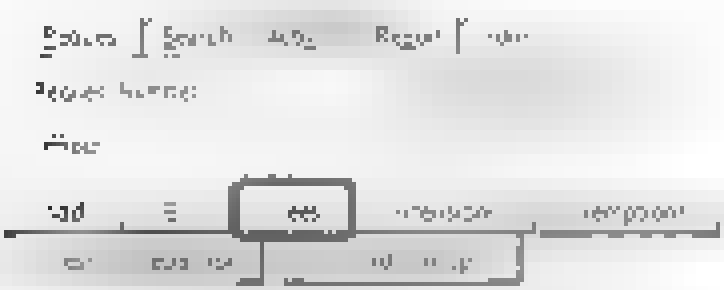
If information is missing to work on the file, such as the SS… or a date of birth, you may insert a NOTE to file (found in … Other) to alert the Analyst information is missing.

5.8 Adding Payment Information for Access to Information Requests

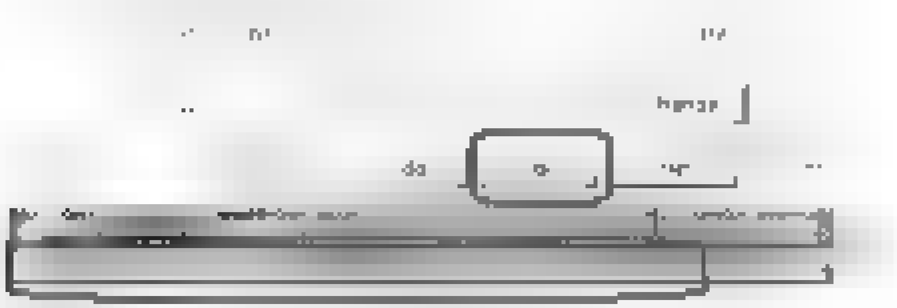
Payment Received

When you receive payment for an access request, do the following.

Open the "receipt" pdf file to get the receipt number (it starts with R…) and in APCM click on the Fees tab.

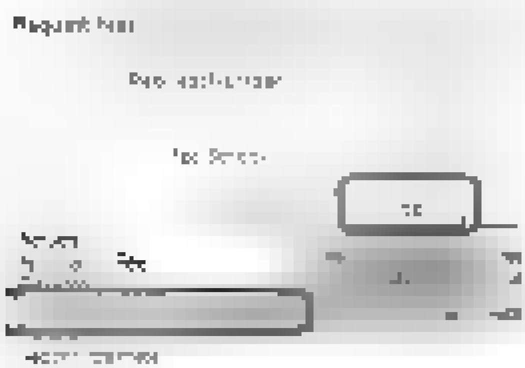


Now highlight the 'Application Fee' action and click **Edit**



Click on "Fee Date" and enter the date that the request was received. For requests received after 4:00pm, or requests received on the weekends enter the following business day. Click **OK**

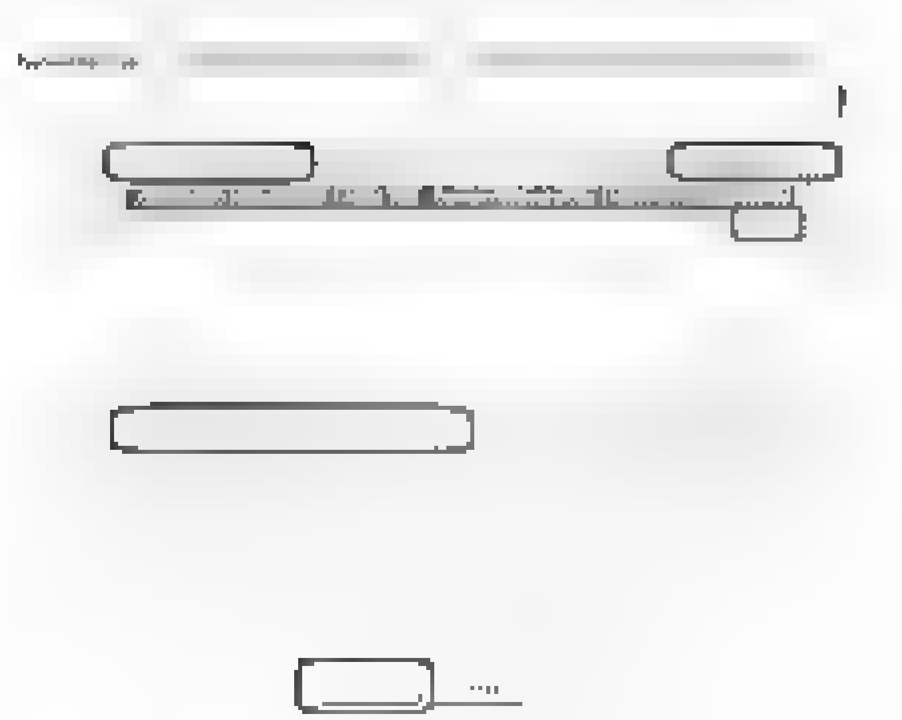
Go back to the Fee screen and in the pull down menu, add the 'Payment Received' action and click **Add**



Change the 'Fee Date' to the same date put in the 'Application Fee' screen. In the Additional Payment field, put 5 for the $5.00 fee and insert the method of payment. In the comments section, type out:

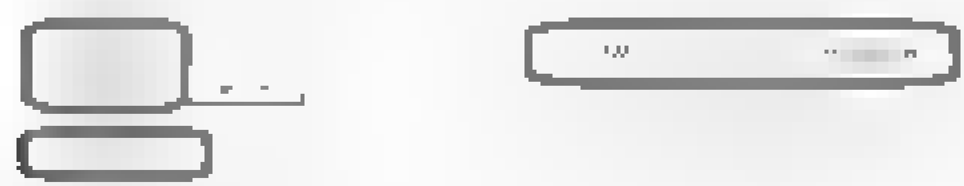
- For online requests type the **RJ210XXX receipt number** and add the following text **'$5.00 Official receipt for application fee'**
- For cheques received type **"$5.00 Cheque #(cheque number) for application fee"**
- For cash received type **'$5.00 cash for application fee'**

And when that is typed, highlight the line and press Ctrl-C to copy the line, then press **OK** and press **Close** to close the fee screen



Go to the actions, scroll to fees and click **Payment Received**

In the Action screen, change the date to the same date entered in the Fees screen, and add the same line added to the Payment Received action by pressing Ctrl-V to paste it, then press OK



<u>**Note.**</u> If the request is transferred from another institution enter the \$5.00 fee as if the request was received directly by us, but add in the comments "Application fee \$0.00, request was transferred from other institution"

6.8 Refunding Payment Information for Access to Information Requests

Payment Returned

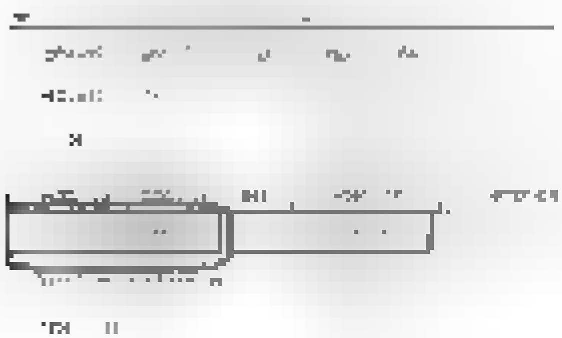
If there is a payment to be returned to the client, the Analyst will open the Payment Returned action in the FEES menu in APCM and indicate the amount and method of payment being

returned file: Date/Analyst Initials - Returning $ - Cheque #XXXX). The action will be closed by the Operations Team during the QCing of the mail out.

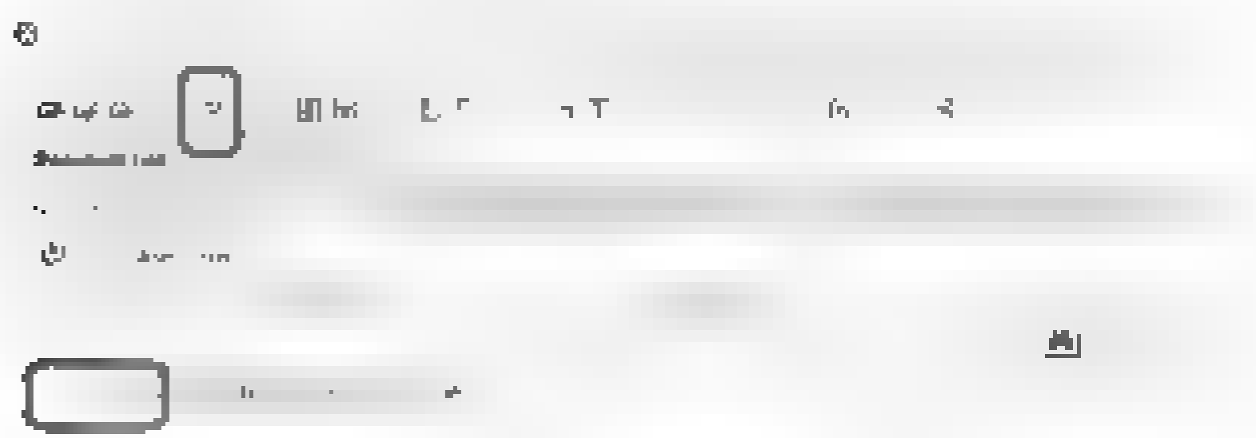
Note: the only time a fee can be returned is if the client applied via regular mail. Online requests do not permit for payments to be returned to a client. If there is a need to return a fee to a client that applied online, please see your Assistant Director to determine if an alternative solution can be found (i.e. giving the client credit towards a future request).

8. ADDING DOCUMENTS IN REDACTION

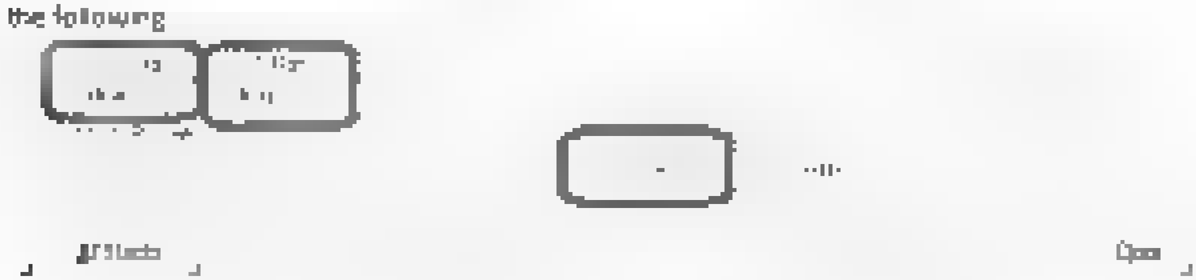
In the action tab, click on **AccessPro Redaction** to open Redaction



In Redaction, click on the **Stacks** button and click **New**



Add the following



Once that is done, for online requests go back to the folder with your files and right click each file to print them to Redaction. Start with the "Request" file, then "Receipt" file, then any other files associated with the request

For hardcopy requests, you can scan these items directly into Redaction

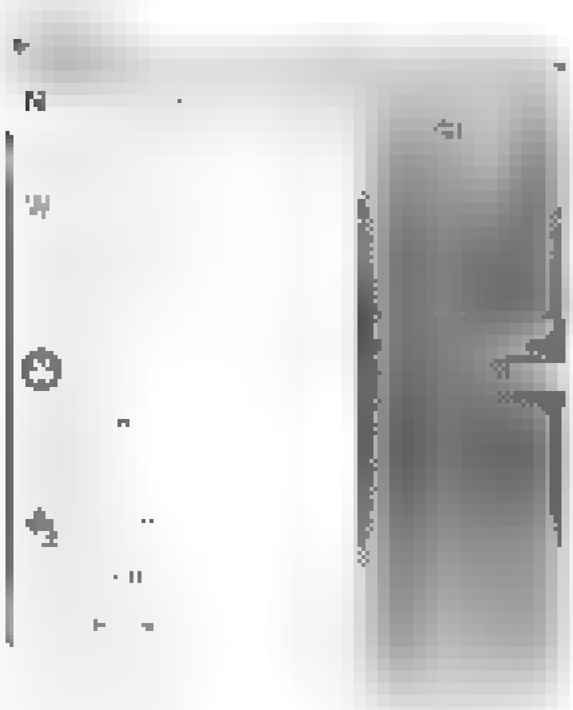
For email, select Print and then 'Print to Image' as your Printer (also see Changing Printer Properties).

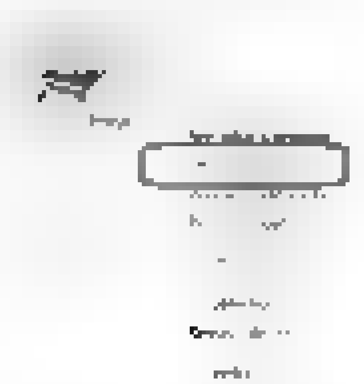
Once your request is in redaction, type 'REQUEST' in the subject of the request file (found under the document index tab).

For online requests, now move the files that you just finished to this month's folder. Now you can go to the next file to open. See ANNEX _ for stacking and indexing standards.

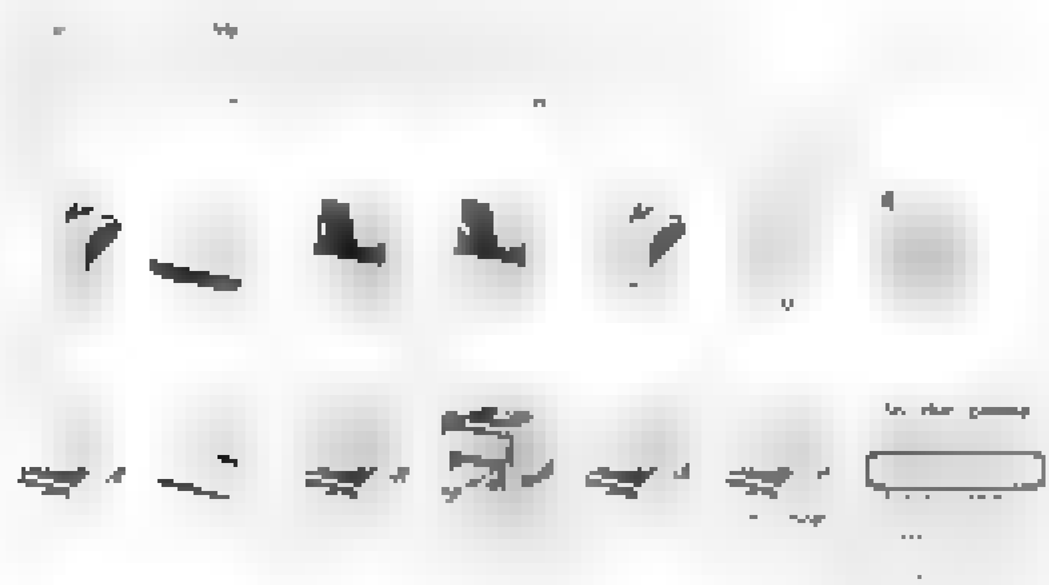
6.1 Changing Printer Properties for Redaction

Go to your printer properties and make **Print to Image** your default printer and change the following settings:

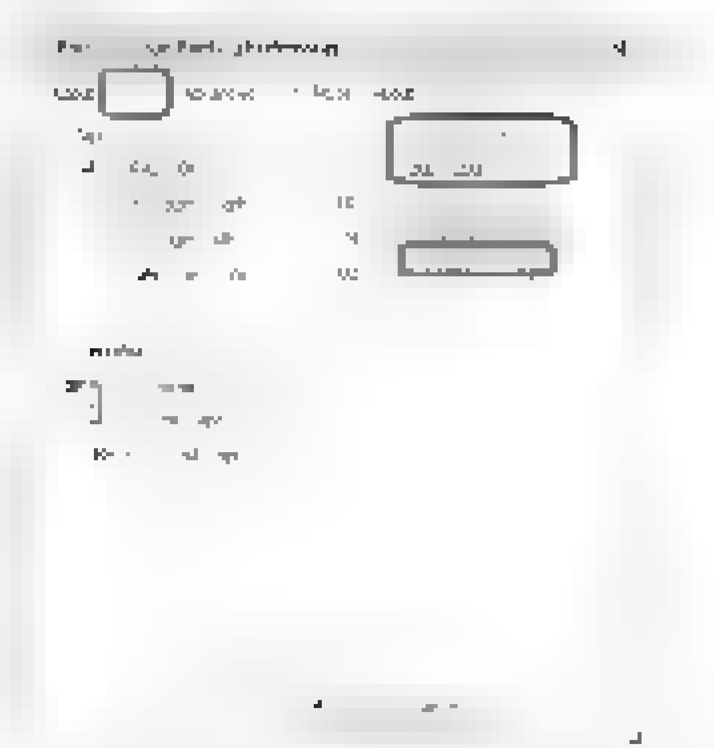




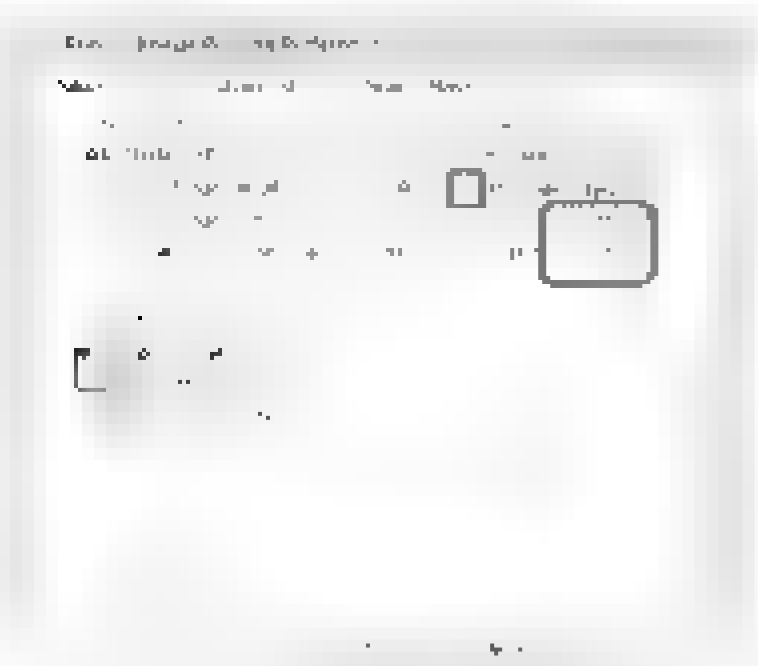
After you set Print 2 image as your default, go to "Printing preferences"



In the printing preferences, go to 'Layout' then change the image resolution to 600x600.



From there, put a check in the Rescale Output box, and change the settings to 300 for each value. Then hit OK



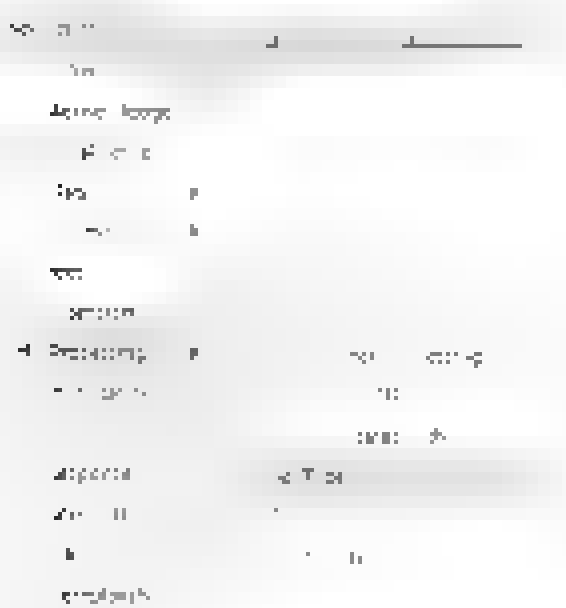
__Note:__ Never under any circumstances, print SECRET or TOP SECRET documents (anything above Protected B) into Redaction. Records that are SECRET or TOP SECRET will remain a hardcopy component of the file until they are treated, and only once the appropriate redactions are made (on our standalone computer or taped) and approved, can the redacted version be scanned into Redaction. See __Annex ‑ Information Classification Guide.__

During the processing of the file, SECRET or TOPSECRET documents should be stored in the appropriate temporary docket and locked in the approved-style cabinet (located in our SECRET room) whenever not in use.

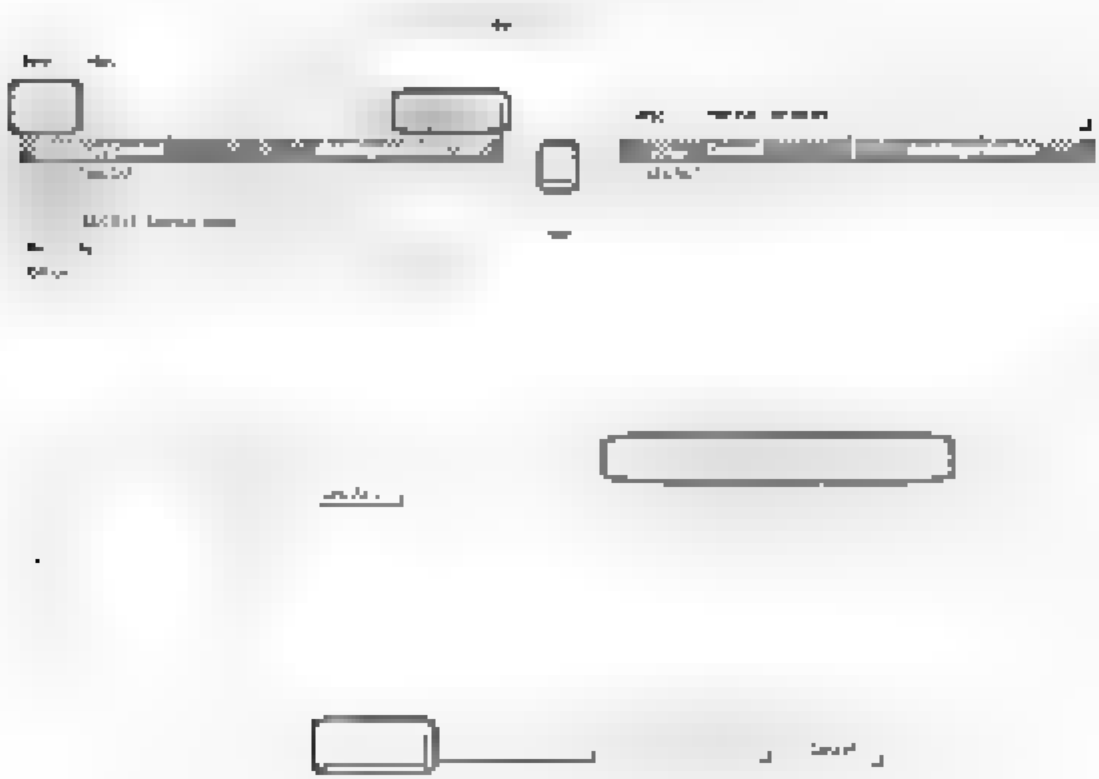
Files with SECRET or TOP SECRET records should be flagged appropriately in APCM, to tell Analysts and Team Leaders that there are additional records other then what is in redaction.

- *Doc Type (h)*

To do this, Add Action "H ‑ Processing" and select Doc Type (h).



By typing "h" into the Name field, and pressing **Search**, you are able to select the relevant document type that is on your file. Highlight the type and press > to bring it over to the right. It is helpful to indicate the number of pages and type of records in the Comments field. Leave Date Completed blank and press **Save**.



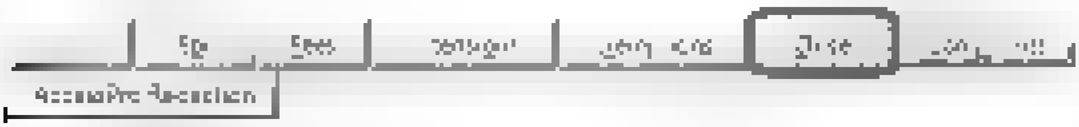
You can also use this Action to indicate when multimedia records exist on your file, such as audio and video. Please indicate the type of multimedia records and their location in the comments field. For more information please see Managing [illegible] Records

7 MAILING OUT AND FINAL QUALITY CHECK

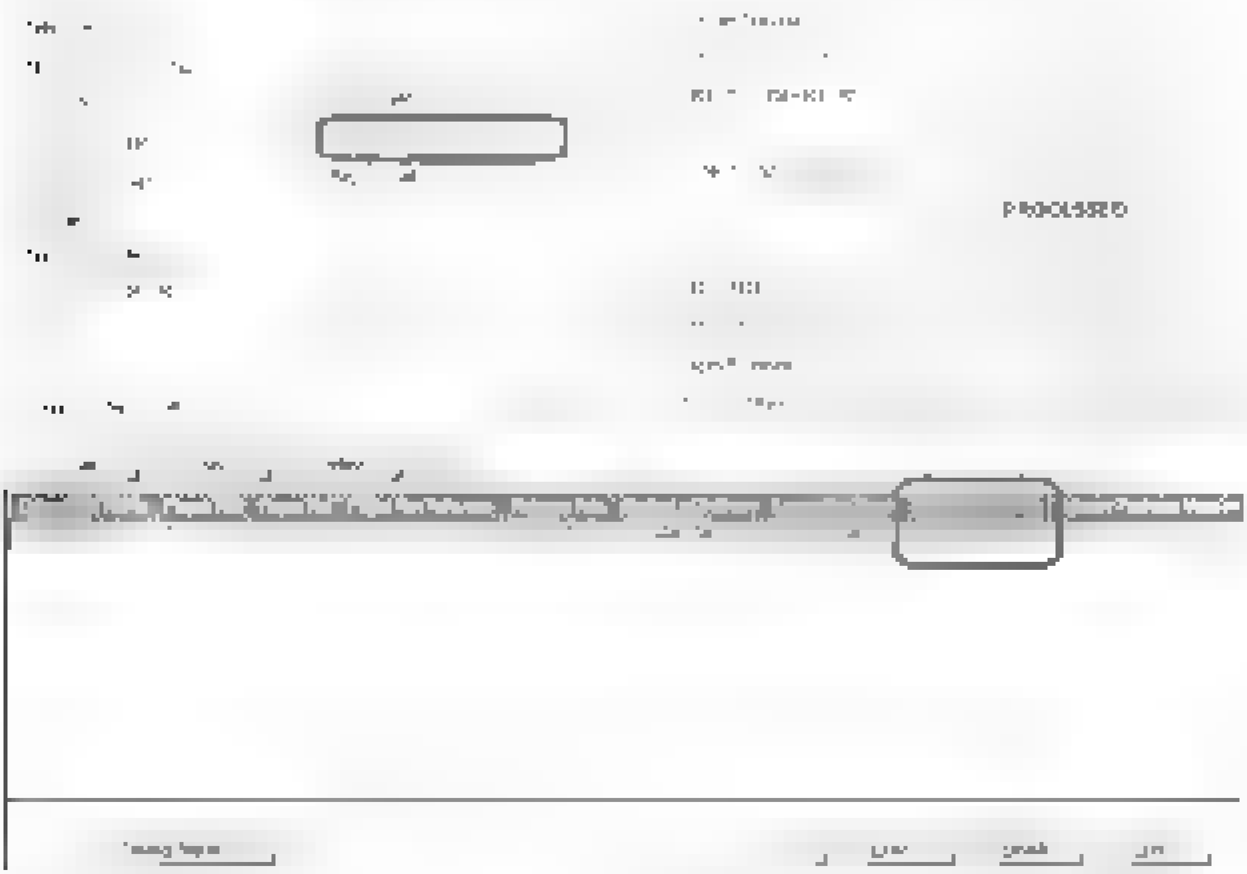
7.1 Regular Mail-outs

Mail outs are located in the following G: drive folder

If you are assigned to do mail-outs for the day, select a file / folder, cut and paste and place it in your own **Mail Out** folder. Open the file number in APCM, and once in the file press **Close** to view the closing screen.



Note the **Method of Access** to determine if this will be a paper or CD mail out. You can press **Finish** now to close this screen.



Your response letter is always a hardcopy, whether or not the applicant is asking for paper or CD. But do not print your letter yet. If this is a paper mail-out, you can go ahead and print the records and once printed, be sure to count the number of pages to what is indicated as released in APCM.

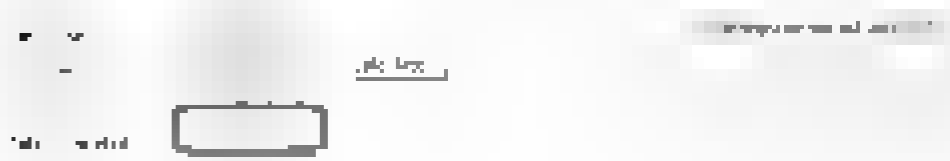
Pages Received:

Pages Reviewed / Released:

Mailed Out

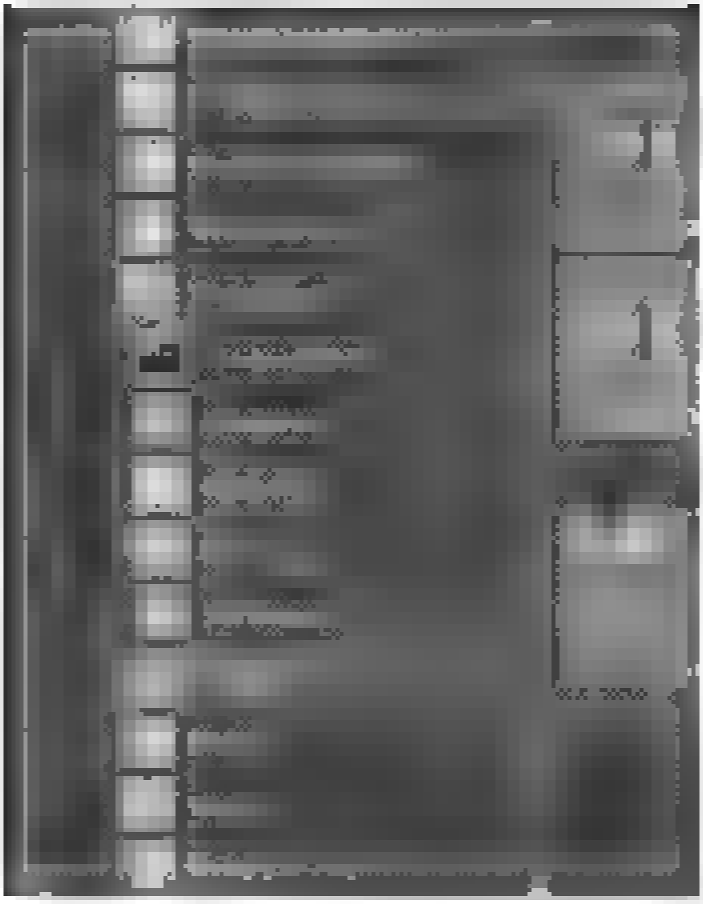
Now in APCM, double click on the **Mailed Out** action line. The Mailed Out action should have been put on already by the Analyst.

Once that box opens, type in your last name in the Name field and press **Search**. Your name will then appear as a contact and you may press > to bring yourself over to the right hand side. Now you may fill in **Date Completed:** as today's date, and type in the comment box "Final response mail out done" and your initial OR "Final mail out with CD done" and your initial (depending on what type of mail-out this was). Now click **Save**.



7.2 Burning a CD

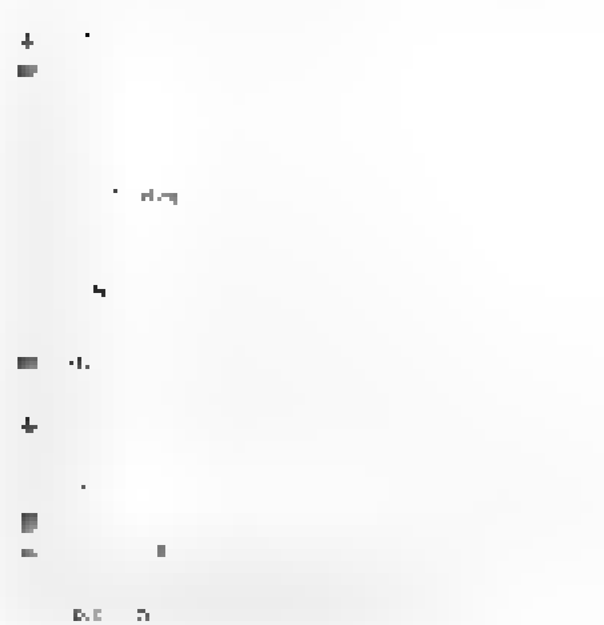
When preparing to burn a CD, open your CD drive and insert your disk. Next, click on the start button at the very bottom left corner of your screen, choose **Windows System**, and then **This PC** and click



The directory will appear

Double left click on the "D:) DVD RW Drive" and the Burn a Disc window will appear. Select "With a CD/ DVD player". The default disc title is the date, but you can substitute an appropriate file title as in the example below A-2038-12345. Then left click on next.

A window will open for the (D:) DVD RW Drive, this is where you drag the file(s) to burn to the CD. Do not burn your letter onto your CD, your letter will be printed on paper.



Once you have dragged or copied the files you wish to burn into the **(D:) DVD RW Drive**, right click on the drive title and a new window will open from which you select (left click) on "**Burn to disc**"

A **Burn to Disc** window will pop up. Click on **Next**.

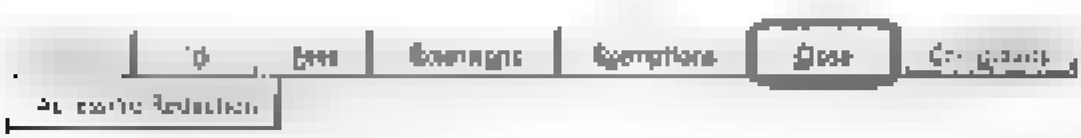
The files will begin to burn to the disc

Once it is finished the CD will eject. Now on the disc write the file number with a black sharpie and put it in a paper protective CD cover. Note: CDs are always to be mailed out with a bubble envelope.

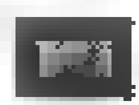
Now go into AccessPro Redaction by simply clicking on the button in the file screen.

Verify the name and address on your printed letter to the name and address on the request. You can also use your label machine at this time to create a label with the person's name and address.

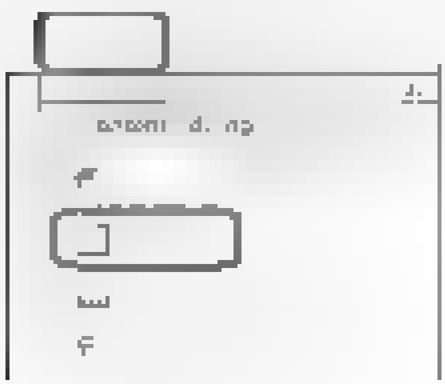
Verify that the Request text is correct on both the letter and again in APCM. Also in APCM, open your closing screen again, by pressing Close.



Now that you have seen the records, verify the Disposition of the records, and whether or not it is "All disclosed" or "Disclosed in part". And press Finish to close.

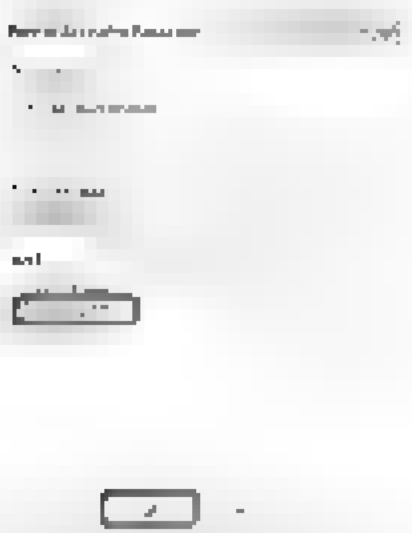


If all everything is verified, double click on your Letter pdf, and once in Adobe, select **Tools** located on the top right. Options on a right hand column will appear below, and now select **Add Text**, and record today's date on your letter, using the format "January 1, 2018", on the top right hand corner of the letter.



Once you have dated the letter, select the drop-down menu **File** and then **Print**. Once in Print, select Printer: **Print-2-Image** and then press **Print**.

A print to AccessPro Redaction box will now pop up. Make sure the correct file number is indicated, and then select the Stack ADMIN before you press OK.



Now that the final version of the letter is in redaction, go into redaction, and type FINAL LETTER in your Document Index Subject field. And press **Save**.

Index Notes

Language ENGLISH

Field

Date

To

From

Subject FINAL LETTER

Save Cancel Click SAVE or CANCEL to continue

Now go back to your Final Letter PDF and also print a hardcopy.

Fold your letter with your records, insert in an envelope (use a bubble if it is a CD) and add a sticky note with the due date and put it in the black cabinet. A final quality check will be done by another person.

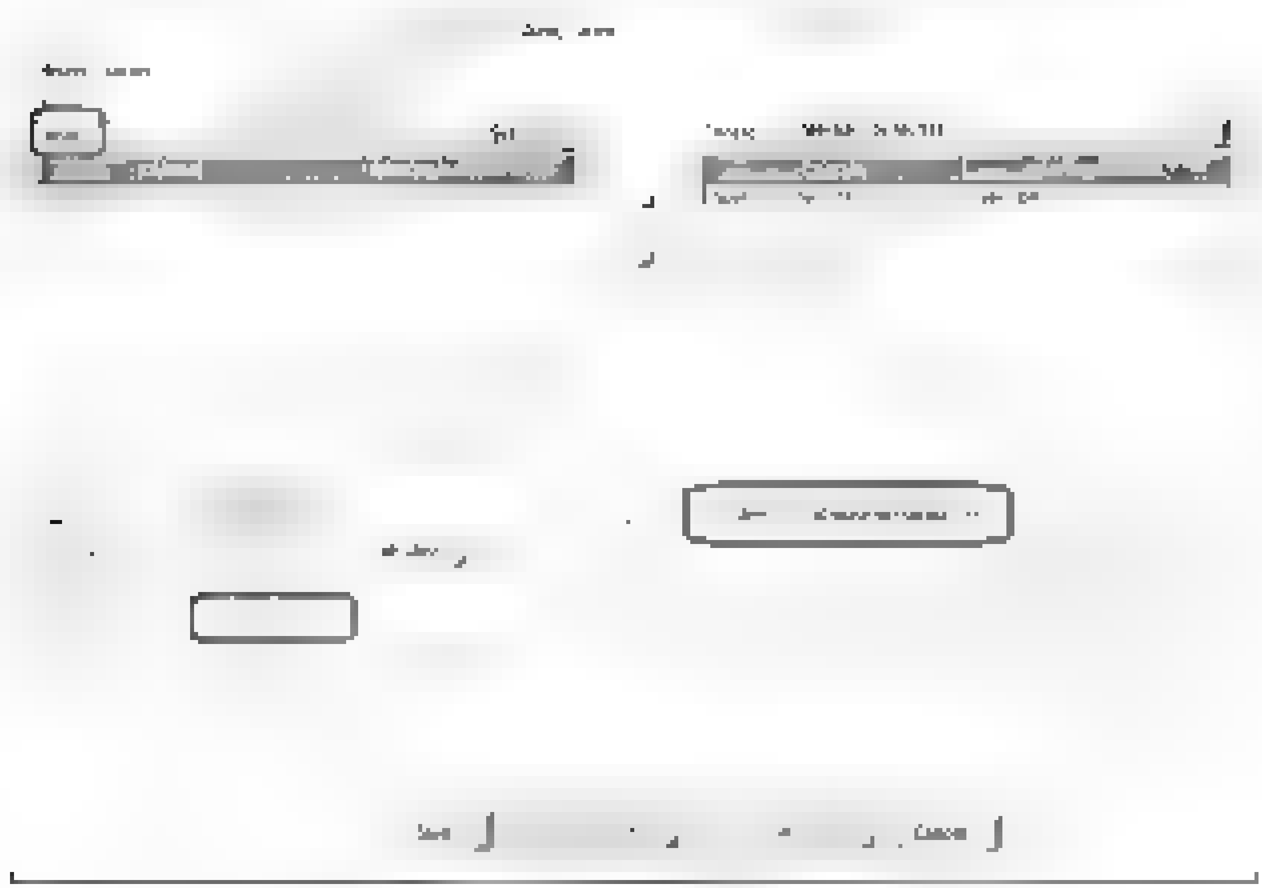
Once the file is complete, drag the file/folder into your own mail out folder, under "Done". You can delete these files after 2 months.

7.3 Final Quality Check

Quality Control

If you are assigned to do final quality checks for the day, you will be responsible to verify in APCM that all the actions have been closed out and to re-verify the accuracy of the address, name, amount of pages and full text to make sure no unforeseen mistakes.

When recording your final quality check in APCM, go to Add Action "M – Closing" and select **Quality Control**. Once in this action box, type your last name into the Name field and bring it over to the right by pressing >. Record date completed as today's date, and in comments write "QC done on final response mail out", and your initial. And press **Save**.



7.4 Courier Mail-outs (Speedy)

Speedy mail-outs are given to the administrative section, either electronically named as CDN-A 2018-XXXX or PC-P 2018-XXX or by paper (dropped off in the designated area in the black cabinet before 11:30am each day). These mail-outs are done the same way as regular mail but the end results is using a Speedy Messenger.

All speedy mail outs are normally for 3rd party consults or mail-outs between government departments. The Address Label maker has the required addresses for these types of mail-outs and is designed to be shared, including any updates made to these addresses. For other government departments always double check the Coordinator's list for any new Director names before printing the label.

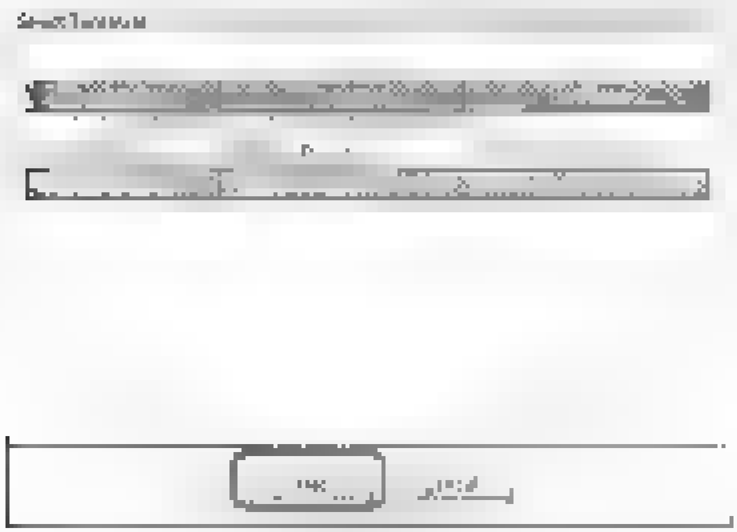
http://www.tbs-sct.gc.ca/hgw-cgf/oversight-surveillance/atip-aiprp/coord-eng.asp

Speedy is called no later than 12:00pm each day for a 2 hour service. If we send off more than 1 envelope to the same person we normally will add on the envelope "1 of 2" and put a rubber band around it and only obtain 1 Speedy LTR for both envelopes.

Any secret documents are to be double enveloped and the inside envelope will have 2 stamps **To Be Open by Address Only** and the **Secret** stamp along with the label address. On the outside envelope will only be the label address. All envelopes will have a written Speedy #. We then hand deliver these mail-outs to the mail room.

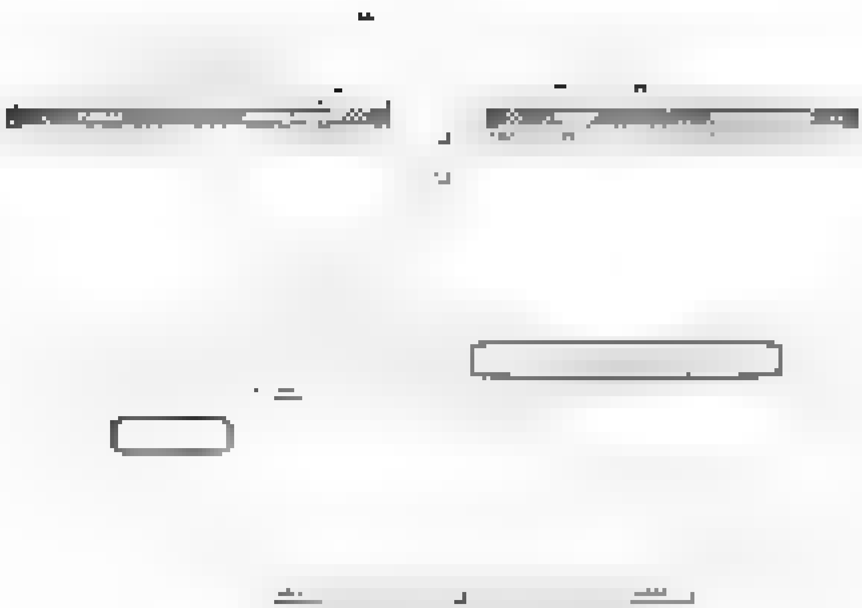
The Mail-out action should already be in APCM for you, inputted by the Analyst. When sending out a consult via speedy, in the comments you should type: mail out to XXX via Speedy TR XXXX and your initial and we do not close this action until a response is received back.

When a response is received we scan the response into Redaction, close the action and write "Rec'd response from XXX" and write today's date and your initial and press **Save**. Next in APCM you will select the consult action that the Analyst had created and then press **Email**, you will be given Template options, choose "Recommendations Received" and press **Select**.



This will generate an email to the Analyst that their recommendations have been received, and scanned into Redaction. Now file the paper copy in the cabinet of the supply room, or if SECRET hand deliver the hardcopy to the Analyst (remember do not scan SECRET documents into Redaction!)

If this is a final mail-out being sent by Speedy we will simply close the mail-out action and in the comment we will type Final mail out via Speedy TR xxx and your initial as below. Again someone will QC this before it is hand delivered to the mail room.

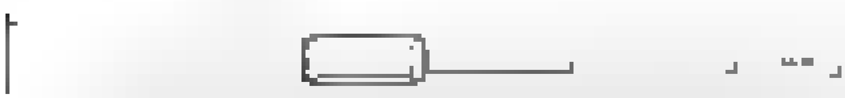


8. RETURNED MAILED

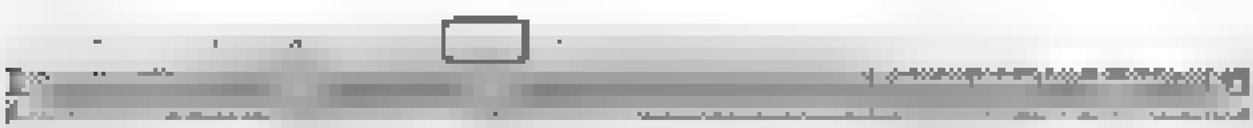
Returned Mail

When we receive returned mail, we date stamp the item on the day we receive it, and then add an action in APCM to record its receipt. To add this action select Add Action in APCM by selecting **E – Response**, then **Returned Mail**

Next write "sent email to clarify address" today's date and your initials in the comment field, put today's date in date completed and press **Save**.



Now in ATIP, highlight and press **Email** to generate an email to the requester to clarify their address.



Once you have proofread the email, add your name to the signature, and press **Send.**

If the applicant does not have an email address specified, please give the piece of returned mail to the Analyst that processed the request. In this case you should write "returned to Analyst", today's date and your initials in the comment field of the **Returned Mail** action. The Analyst will contact the requester and clarify the address themselves. Once they have done this, they will provide the new address and create a new Mail-Out Action for the administrative team.

PRODUCTION UNIT SECTION

9. TRANSFERRING AN ATIA REQUEST TO ANOTHER GOVERNMENT INSTITUTION

When an *Access to Information Act* (ATIA) request is received, one of the first steps as an Analyst is to verify that the information being requested is under the control of the government institution receiving the request. If the information is under the control of another government institution, the request can be transferred within 15 days from the date the request is received.

The ATIP Coordinator of the other government institution is contacted to obtain his or her agreement for the transfer. The requester is then advised in writing that the request has been transferred on his or her behalf.

The 30 day time frame for the other institution starts from the date we received the request, not from the date the other institution received it from us. So it is imperative to action the transfer as quickly as possible.

Should it be determined that the information being requested belongs to another government institution after more than 15 days from the day of receipt, a letter re-directing the requester to submit the request to the other government institution is issued and the file is closed.

Requests made under the *Privacy Act* cannot be transferred. If the CBSA does not have the information requested, the requester is advised in writing and the file is closed. Should it be apparent that another government institution holds the information, the requester is advised accordingly. If the request was obviously misdirected to the CBSA and the requester agrees, the request is forwarded to the appropriate institution on the requester's behalf.

10. ASSIGNMENT OF A FILE TO AN ANALYST

Once the requests have been entered into APCM, they can be found in the "NEW REQUEST NEW REQUEST" or [illegible] "New Requests" folders.

The Administrative Manager should review the new files. In the [illegible] screen they confirm the accuracy of the following:

- Request text in APCM
- Requester's name and contact information
- Source
- Category
- Verify dates (date on request, date received, complete received)

Additional actions are then added, where required:

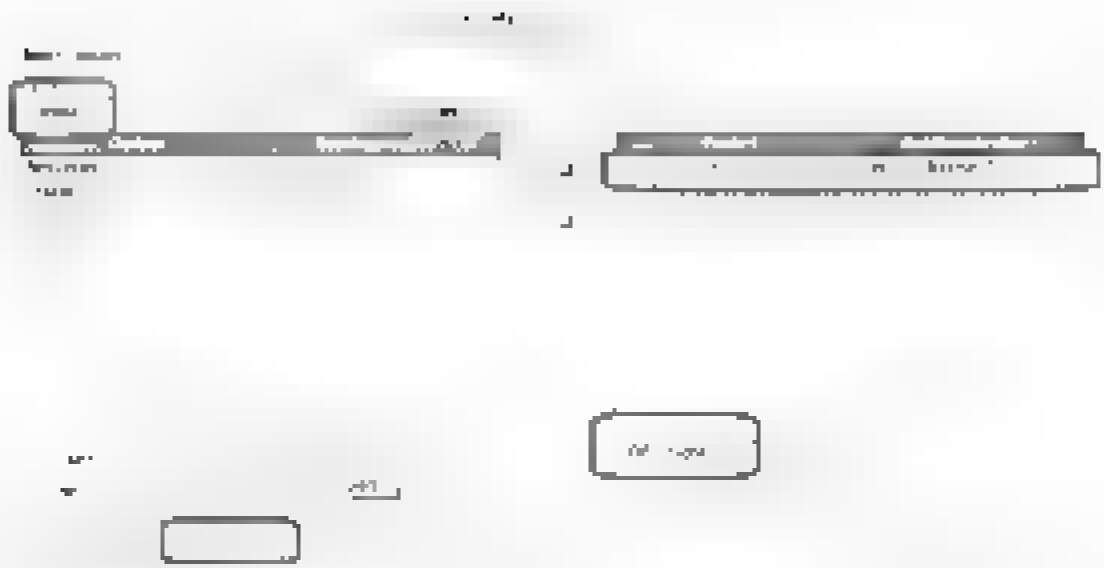
- Deleted from Retrieval Folder (located under M[illegible]keying)
- HEADS-UP, [illegible] to (for [illegible] Access, type [illegible] in the name field and press **Search**):
  - ATIP Director (Director's Review Meeting)
  - Briefing Folder Copy (Expect release package on the [illegible] CBSA ATIP Briefing folder)
  - COMMUNICATIONS (COMM's review)
  - Briefing Folder Copy (used in conjunction with COMMUNICATIONS)

The Administrative Manager will then divide all files in the [illegible] "New Requests" folder to the PM-01s folders in each team's tree (these are labelled "PM-01 New Requests"). The PM-01s are responsible to grab all Travel History requests from this folder, and move them into their "name" folder.

The Administrative Manager will then divide all files in the "NEW REQUEST, NEW REQUEST" folder to the 3 Prod folders (Production A, Production B and Production C). Each Prod folder has its own "New Requests" folder. Each Assistant Director responsible for that specific Production unit will then split the files amongst their Analysts using the **AssignReview** action (located in [illegible] Initial Setup).

AssignReview

The Assistant Director will need to search the last name of the chosen Analyst in the Name field and then select their name, and press the > to bring their name over to the right. The Assistant Director should also place their initials and "Assigned" in the comment box as shown below and the date completed as today's date.



SPECIAL INSTRUCTIONS

At this time special instructions can also be added by the Assistant Director if required. This action is under Other.

Each Analyst is expected to monitor their team's **New Requests** folder and capture the files assigned to them as shown in the **AssignReview** action, and then bring the file into their own folder for their review.

AssignReview

The **AssignReview** action (located in B. Setup) can also be used by the Assistant Director in any instances that the file needs to be transfer from one previously assigned Analyst to another.

Once a file is assigned to an Analyst, the first thing the Analyst should do is review the request to ensure it's complete and ready to be processed. The following questions can be asked:

- ⇒ Is it clear what information they are looking for?
  Has this same request been made before? For Access requests perhaps we have done this request before and this can be responded too informally.
- ⇒ Is the request text correct and clear and any personal information in privacy brackets
- ⇒ Is the requester's address complete?
  Do they have a Right of Access?
- ⇒ If an Access request, have they paid the $5.00 fee?

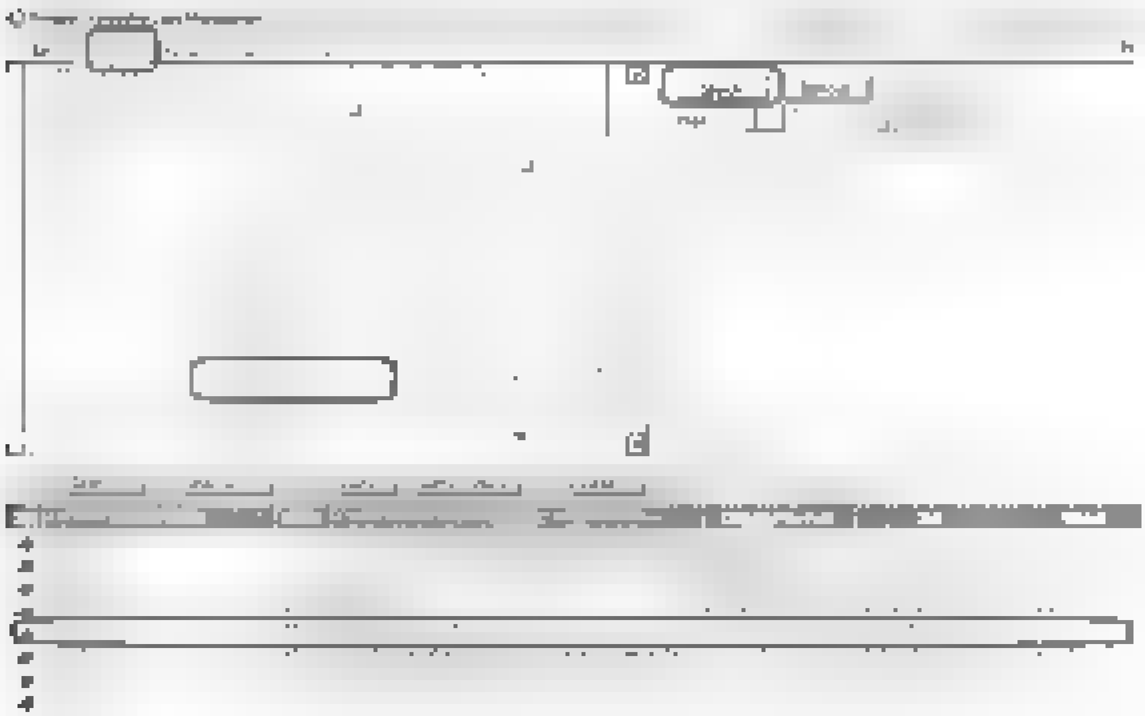
- Is the scope reasonable to provide them the information in a timely manner? Can it be down scoped? Or re-scoped to provide what they are seeking in a more timely manner?

11 SEARCHING FOR CROSS REFERENCES

Cross-Reference

This step was also done by the admin section, but is an important step to be repeated by the Analyst.

Looking at the request, you will want to do a quick search in APCM to locate any cross-references there may be. Locate any key words in the text (ie. a person's name, or FOSS or ENT ID number, or if it is not for personal information a key term being used like "Enforcement Manual") and search those words in the "Full text" area in APCM.



If a cross-reference is found and the action isn't already present in your file, to add the action select "B – Initial Set up", then **Cross-Reference** and note the relevant file number "A-2017-0XXXX/CUD" in the comment box including the initials of the Analyst that processed the file. Do not add any other information in the comment box.

When recording the cross reference, for individuals write all the file numbers down. For generic terms, use your judgement, but if it is generic like the enforcement manual, just include the most recent file number.

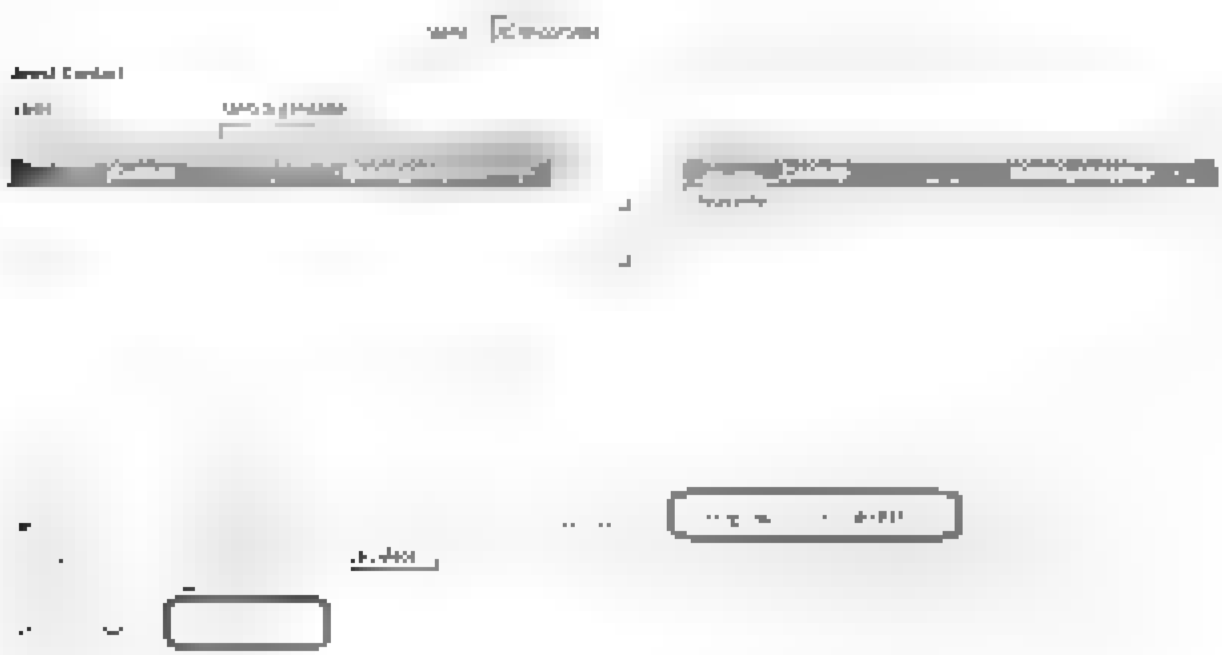
If the requester is seeking the same information as a previous file (i.e. The enforcement manual) it may be possible to respond to the request informally by offering the client a copy of that previous request.

12. ACKNOWLEDGEMENT INCOMPLETES (if required)

ACKincomplete

Once you have confirmed the request is not a duplicate request, you can look at if the file requires more information or a clarification in order to be processed. If this is the case, the Analyst can use the action **ACKincomplete** (found in A – Acknowledge) to put the request on hold and a letter or email is then sent to the client requesting the information or clarification required.

The Analyst should also indicate in the comments section as to the reason the file is being placed on hold and the "date completed" will remain blank until the information is received. The **ACKincomplete** is only used when the action is necessary in order to process the file, and once you have added the action and appropriate comments indicating the reason it is incomplete press Save.

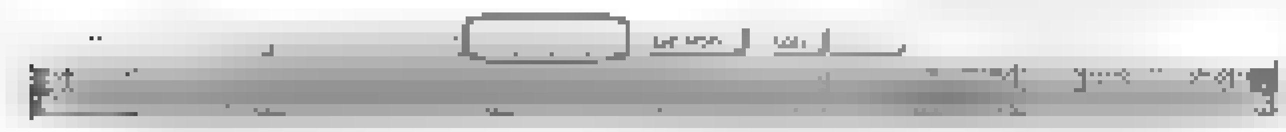


Furthermore, if a request is too broad, or unclear, the Analyst can contact the client to clarify or narrow down the request. For example, if a client wishes to have a copy of all emails sent and received by the President of CBSA, we would go back to them to provide us with a date range and specific subjects, otherwise the request would be tens of thousands of pages of material, much of which would not be releasable. Although people have the right to ask for information, the requests cannot be frivolous and impede the workings of an office. So we use **ACKincomplete** in this instance as well.

For those requests lacking consent, the form can be found at the following location bsf745 for English and bsf745 for French. It is also available online at the following website: http://www.cbsa-asfc.gc.ca/publications/forms-formulaires/bsf745-eng.html

Note: If you call the requester for more information/clarification, use the ACKIncomplete action to place the file on hold, but after three days generate the appropriate letter or email, to put your request in writing. Do not abandon a request without having sent a letter or email offering the requester 30 days to respond.

Now you have created the ACKIncomplete action, you will want to select that line, and press either the Email or Letter button, whichever format you will send.



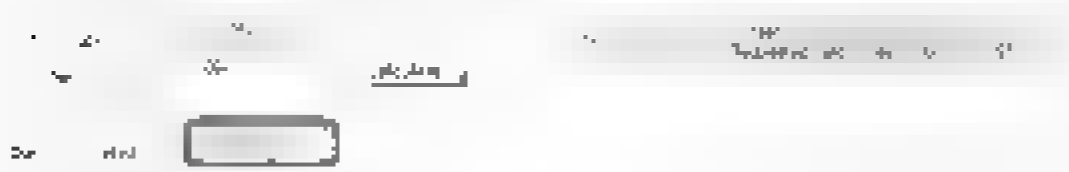
When either the letter or email pops up, you will want to do the following:

Letter	Email
1. Remove "CANADA" from the address 2. Delete "Your file" at the top 3. Fix the name of requester so it's Mr. Last name or Ms. Last Name (when they don't identify themselves as a Mr. or Mrs. Use their first name + last name) 4. Remove the privacy brackets [ ] from the summary 5. Insert missing information blurb (see Appendix D) 6. Print and sign 7. Now add a mail-out action in APCM (found under MI - Closing) and record "sent for mail-out" with today's date and your initials in the comments field, and leaving "date completed" open	1. Fix the name of requester so it's Mr. Last name or Ms. Last Name (when they don't identify themselves as a Mr. or Mrs. Use their first name + last name) 2. Remove the privacy brackets [ ] from the summary and edit this text to be clear of any Protected B information, as it will be sent by unencrypted email 3. Insert missing information blurb (see Appendix D) 4. Send the email 5. Print 2 image the email to Redaction from your sent folder in Outlook

12.1 When the Missing Information Is Received

Once the missing information is received, either the Administrative Team will have printed the information for you into Redaction (if received by mail) and notified you of its receipt, or you can print the response into Redaction yourself if received by email. Please modify the request in APCM where applicable once you have clarification. Double click on your ACKIncomplete line

in APCM, and insert the **Date Completed**, inputting the date you received the information. If you received it after 4pm on a business day or on a weekend, use the following business day. You may also insert a note in the "comments" section pertaining to the action. Once completed, press **Save** and you can proceed with the file.

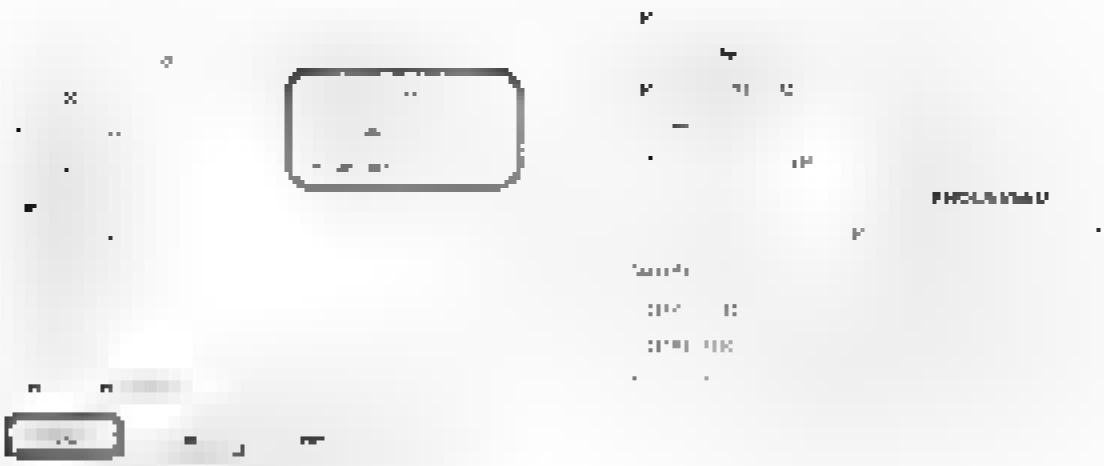


12.2 Closing an Abandoned File

A client is given 30 days to respond to the **ACKIncomplete**. If no response is received after 45 days (we use 45 days as a courtesy), the file is considered abandoned by the client and is closed in APCM. To close you, you can enter the date completed to today's date, and place in the comments field "considered abandoned after Xx days", today's date and your initials.

After the **ACKIncomplete** action is closed, next you will want to click on **Close** in APCM.

A Close Request box will pop up. You now want to fill in the following sections: Disposition (select – Abandoned by applicant), Method of Access (select – Not Applicable), and Method of Delivery (select – Not Applicable). Once finished press **Add**.



Fill in the sections as shown below. Release Date should be today's date (the date you are closing the file). And press **Finish**.

Disposition	Abandoned by applicant
Pages Reviewed	
Pages Released	
Pages Not Released	
Method of Delivery	Not Applicable
Translation	Not Applicable
Method of Access	Not Applicable
Release Date	[illegible]
Fee status	Completed

You will see it as a disposition line in the Close Request box now.

Lastly, enter the Date Closed and Date Communicated to today's date. And press **Finish** again. The file should no longer appear in your tree.

VERSION 10

Date issued	26-06-20
Next review date	26-06-2018

[illegible]

[illegible]

After an Analyst determines that a request has enough [illegible]

[illegible] determine which of its CAT(s) should be sent the tasking

[illegible] Analyst to vet

[illegible]

[illegible]

Information on how to process each type of request is further described below

13.1 Travel History Requests

Travel History (TH) requests are clients seeking a list of their entries and/or exits in/out of Canada. These requests are being handled entirely in-house as the ATIP Division has access to ICES and COGNOS, which both track this information.

Your first step, once you have been assigned a Travel History file is to review it for completeness (please see section: Acknowledgement (incomplete/if required))

Some common reasons a TH file would be considered incomplete are:

- No date of birth
- ⇒ No travel document provided (Passport, Permanent Resident Card, etc.) or Client ID #
- ⇒ No valid consent
- No parental consent for a minor (Under 16, or 18 for use of representative)
- ⇒ No right of access
- ⇒ Request is not clear

If the file has been pending any of this information, and it has since been received, print the missing information into Redaction (if received by email). If the information was received by mail it should already be in Redaction waiting for you. You may also need to modify the full text and summary text in APCM to include the missing information.

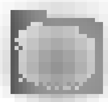
13.1.1 Using GCMS for TH Requests

You can use GCMS to find additional travel document numbers that you can use when running your TH Reports, such as Passport numbers and Permanent Resident Card numbers.

To log into GCMS, follow the IRCC log in screen located here:

To log into Citrix use your Citrix ID along with the password associated with your Citrix account.

Once the IRCC page opens up, you will see 4 folders, click on the GCMS folder.

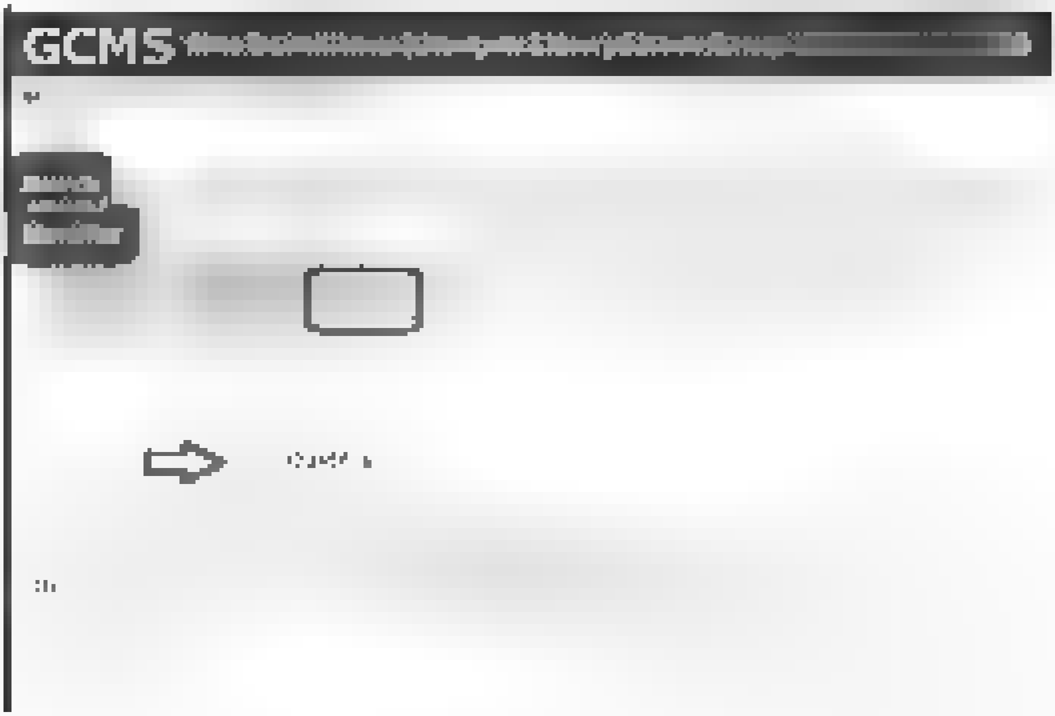


Next, click on the GCMS – Chrome icon

Your ID to access GCMS is   and your password is the same as the one that you used for Citrix

If you do not have the Client ID to search for your client in GCMS, go to the **Search** tab and then the **Integrated** tab. Fill out the family name and given name and DOB if you have it (enter it as YYYYMMDD) and press **Search**. Wait approximately 5 to 10 seconds and then press the refresh button. If the search is slow, wait a few more seconds and hit refresh once, twice or three times and it should finally generate a list of possible matches.

If you do have the Client ID, you can click on the **Identifier** tab, also under the Search tab, and search for them using it. To do this, in the "Type" box select **UCI/FOSS ID** in the drop down menu, and once the Client ID is entered, press **Search**.



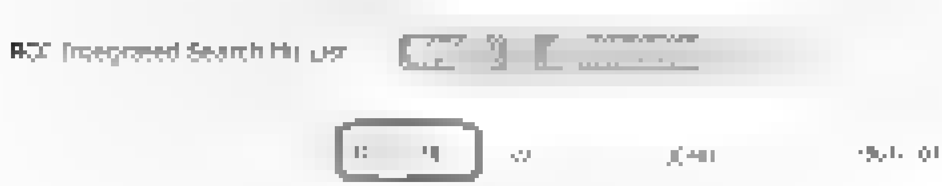
Once you have pressed Search, either your client, or a list of clients will populate below at the **IRCC Integrated Search Hit List**. You now need to verify that the family name, given name and DOB match up with the request. If they do not further clarification will be required.

Next click on your client and then the **Client Detail** tab. Here you may find FOSS Personal Details on your right, and within a Passport number. This area will also include any Aliases you may want to search (if they exist). You will need to press the "Get FOSS Details" button for the information to appear. If the "Get FOSS Details" button is greyed out, the Client Detail and FOSS PRs won't exist. If FOSS Personal Details exist, do a screen capture of this section, paste your clipping into Word and then Print it into Redaction.

The next tab that you will want to search in is FOSS PRC. If the client has a PR card, the PR number should be recorded here.

The last tab that you will want to search in is the Docs tab. It may contain additional travel documents that weren't displayed in the previous tabs.

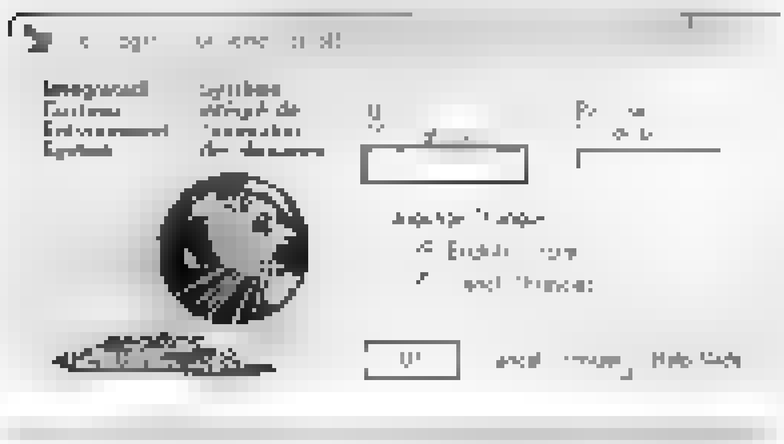
The last place to look is the Client Section. To find this area, click on the Client ID number in the **Integrated Search Hit List**, and the client section will open.



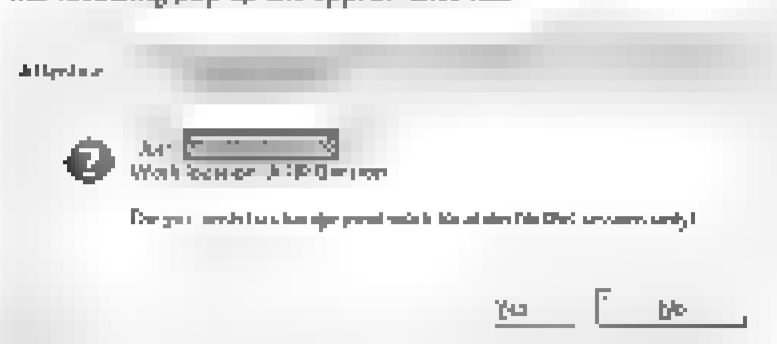
In the lower area of the Client section, click on the **Documents** tab. Here you will see a **Travel Documents** tab as well as a **IRCC Documents** tab. These tabs may have additional travel documents. If you find any additional document numbers, it is important to add them to your word document that you will print into Redaction.

13.1.2 Running a TH report

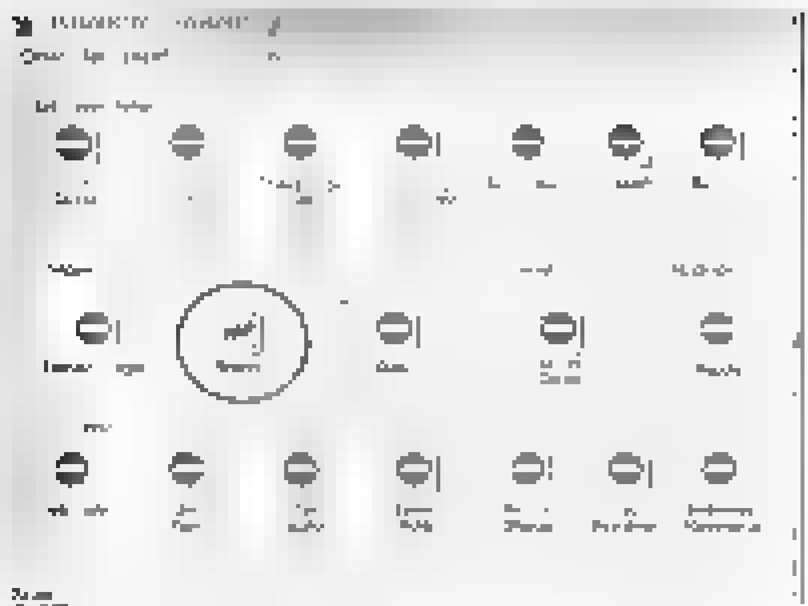
Now, you will want to open ICES on your computer. Type in your **User Id** and **Password**. If you have a French request, remember to change the language before you log in. Changing the language to French will generate a French report.



The following pop up will appear, click **No**.

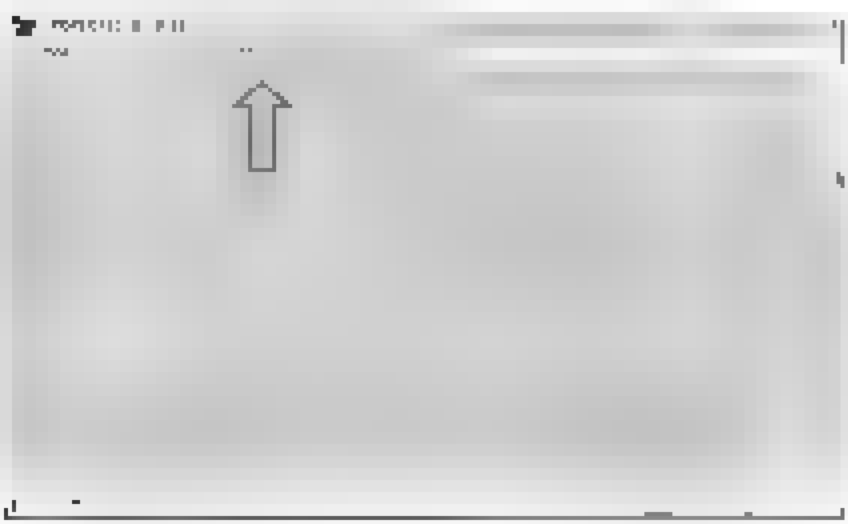


On your next screen click **Reports**.

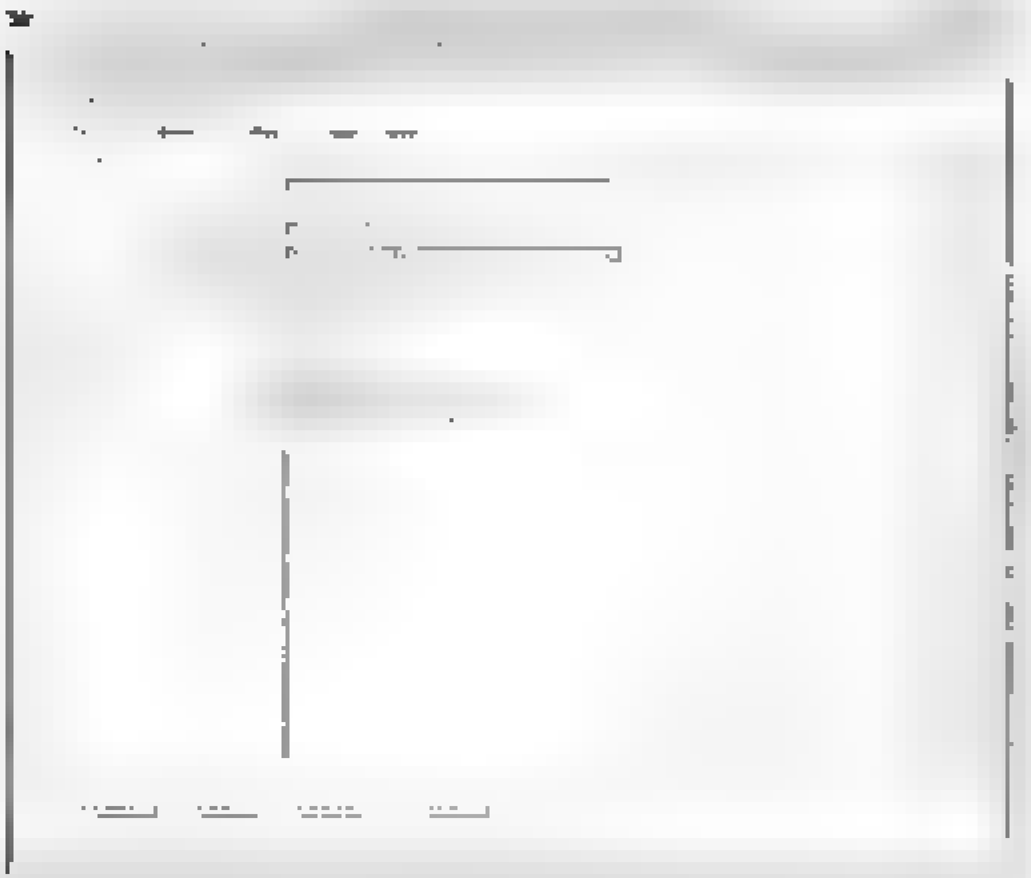


The ICES Reporting screen will now open. Press on the **Traveller History** drop down and choose the option **ATIP Travel History Report**.

Note: For immigration file requests we automatically provide the Full Travel History Report. For this you will select **Traveller Passage Report** instead of **ATIP Travel Passage Report**. This will produce a report that contains additional columns of referrals, Doc. Type and Property Codes.



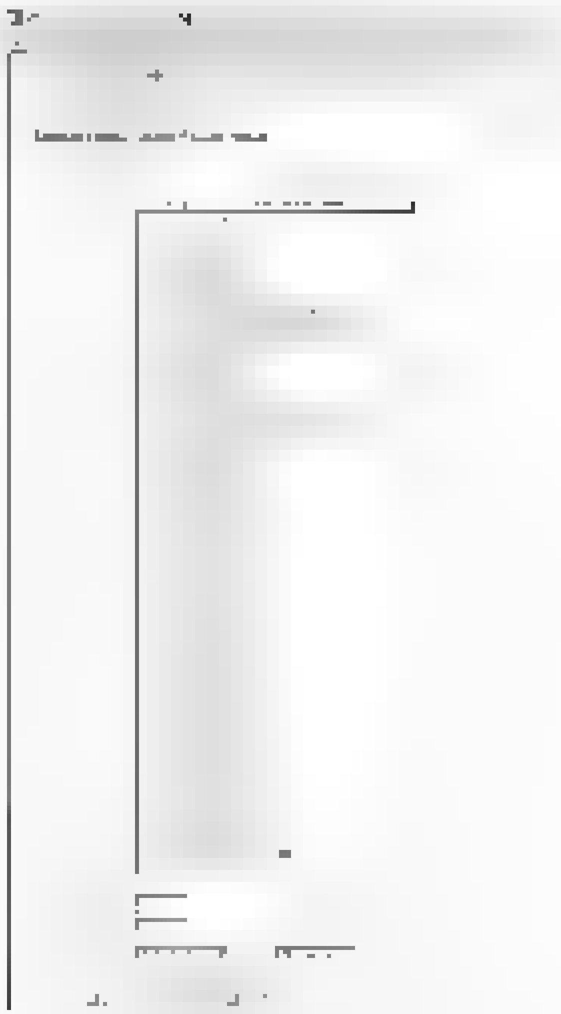
Once the **ATIP Traveller Passage Report** screen appears, you will enter the information pertaining to the client. The **Last Name** must be entered in its entirety; for the **First Name**, try to search using the first few letters of their name (if possible). Often names are misspelled, and this will ensure that you capture as many entries related to the specific individual as possible. DOBs are entered YYYY/MM/DD. Leave **Exact Match** X'ed.



Now click on the **Details** tab (at the top). Fill out the date range as requested by the client. If no start date was provided, or if they are asking for all dates, the start date will always be August [illegible] 2000, as it is the earliest date that we can retrieve. The dates are entered YYYY/MM/DD. Times should always start at 00:00 in the **From** box and end at 23:59 in the **To** box.

In the **Details** tab, you can also select specific work locations, should the client be seeking entries related to a certain point of entry. Hold down **Ctrl** when making selections of several locations at once. When there is no specification on the point of entry, there is no need for this step.

Once you are done with these steps, click **Proceed**.



Now that your Travel History report is generated, take a quick glance and see if you need to add more letters in the **First Name** box to eliminate incorrect entries in your report. If you want to add more letters to the **First Name**, go back to the **Travellers** tab, add the letters and press **Proceed** again.

Once your report is satisfactory, Print it to Redaction. Make sure that your printer's default setting is set to "Print to Image" and that the resolution is at 600x600. For more details on this step, review Changing Printer Properties for Redaction.

On the Document Index of the GCMS word docket (in Redaction), type in all of the document numbers that you have found in ICES and record the number of entries found for each document. Now record any additional travel document numbers that you have found earlier in your GCMS search, as well as the ones provided by the requester. You will want to cross reference the entries in your report, using each travel document number that you have inputted in the Document Index.

To do this verification, click on the **Traveller** tab again. At the bottom of the page, click **Clear** to remove the Traveller's name and DOB. Now, type in one of the document numbers into the **Document Number** field and press **Proceed**. This will generate a report for that specific travel document. Count the entries related to that document, and cross reference it with the number that you had recorded from your initial report. You will repeat this step for all of the travel documents that you have inputted. This verification will catch any additional entries that the initial report had missed. As you verify each document, you can place an * beside the number in your list to display that you have performed a verification.

If you catch any additional entries, print that new report (showing the additional entry) into Redaction as well. It is also good practice to highlight the types in Redaction with the yellow highlighter for your Team Leader. These additional reports must also be provided to the client. It is common to provide the client with more than one report when necessary.

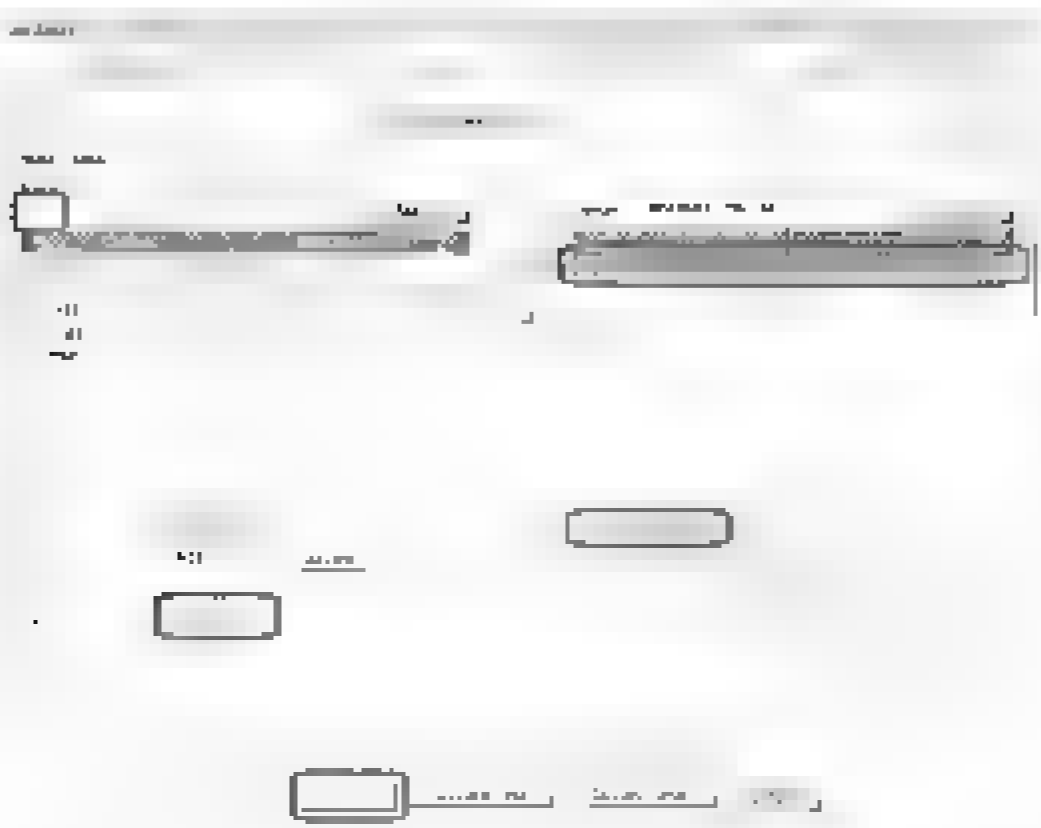
Once your Travel History Report and verification are both completed, go back to your file in APCM.

SYSTEM NOTES (e).

Add the ICES Action to your file by going to **Add Action**, selecting **E** [illegible] **Retrieval** and **SYSTEM NOTES (e)**.

In the SYSTEM NOTES **Name** field, type in 'c' and press **Search**. Select **NOES** and press > to bring your selection to the right hand side. Type TH done todays date and your initials in the **Comment** field. Put today's date in Date Completed and press **Save**.

If no Travel History entries were found during your search, type 'NIL' in the **Comment** field. Put today's date in Date Completed and press **Save**.



13.1.3 Exit Reports in COGNOS

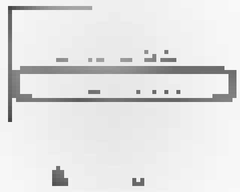
If a client is also seeking their exits, you will need to perform the following additional steps below. Exits are provided to us through an information sharing agreement with US Customs. Exits are not tracked in ICES, they can be located in COGNOS.

First you want to open COGNOS.

If you have *already created a shortcut for COGNOS please* *[click here](#)* *to proceed*.

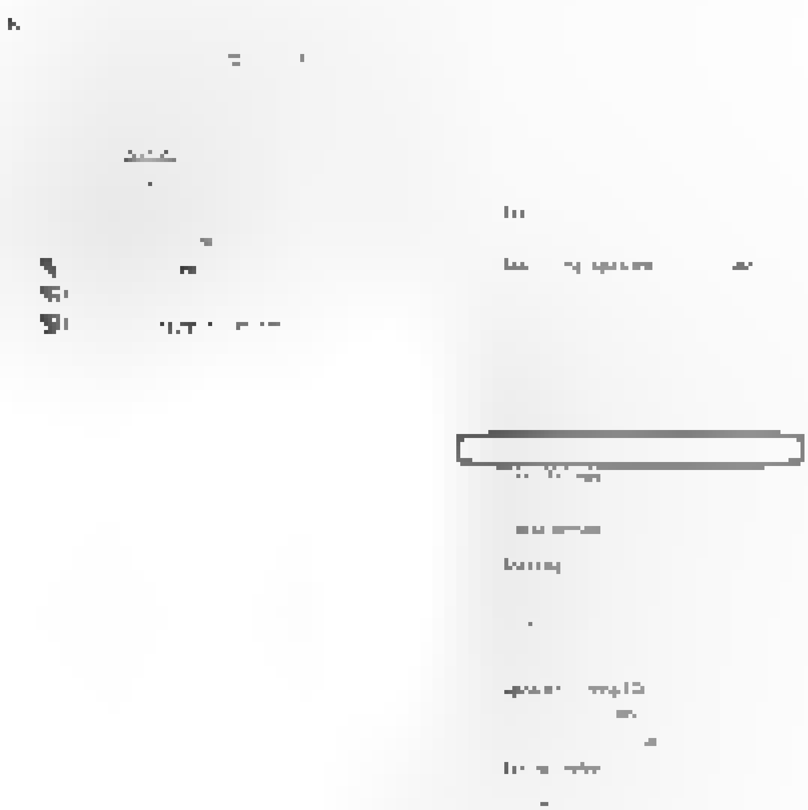
Once it opens in your web browser, click on **My home.**

Select the **Language** in which the report will be done in. Once the language has been selected, folders will appear. You will want to select **10+ Travellers.**

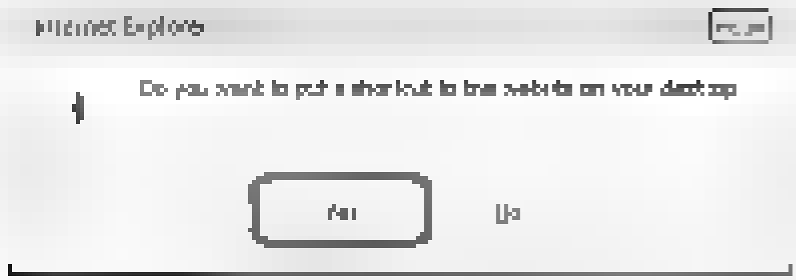


Now the folder **90 – Entry and Exit** will appear. Click into that folder, and then again onto **10 – ATIP Requests**.

It is helpful to create a shortcut for this screen onto your desktop. To do this, right click anywhere on this page and select **Create shortcut**.



When the pop up box appears, select **Yes**.



The shortcut will now appear on your desktop under the name **Public Folders - IBM Cognos Connection**. You can rename the shortcut if you wish. To this, right click on the icon and press **Rename**. It is helpful to create a shortcut for the report in both languages.

Firstly, you will adjust the date range in the report.

ATIP Requests

From

To

From:

We only started recording Exits on June 30th 2013. For this reason, if the requester asks for a date prior to June 30th 2013, the start date will remain June 30th 2013.

If the requester asks for a date after June 30th 2013, we use the start date stated on their request.

To:

The end date for the exit report may be a specific date given by the requester.

If the requester is asking for all dates, we use the "Date Complete Received" in APOM as the end date for the report.

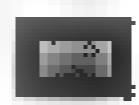
Next, insert the complete **Last Name:** of the requester and **Record Type:** select Exit

Last Name:

Record Type: Exit

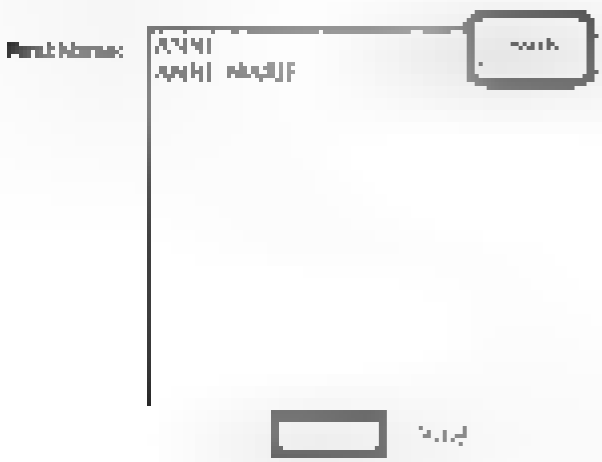
For Date of Birth: modify the Year, Month and Day to correspond with the Client's Date of Birth

Click **Next** at the bottom of the screen



The CBSA began collecting traveller exit information on foreign nationals (excluding U.S. citizens) entering the United States from Canada on June 30, 2013. As of July 11th 2019, the CBSA collects exit information on all travellers (including Canadian and U.S. citizens) at land ports. It is common that no exit information exists. If this happens, the next screen will show no first names.

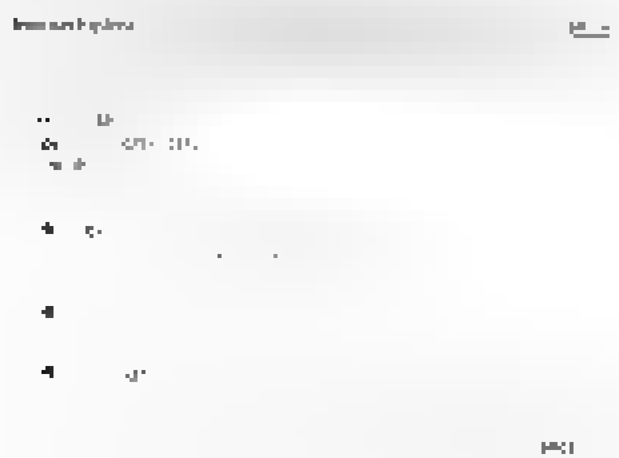
If exit exists, one or more first names will appear on your screen. Click on the first name(s) that correspond with the client. If all names correspond, you can press **Select all** and then press **Search**.



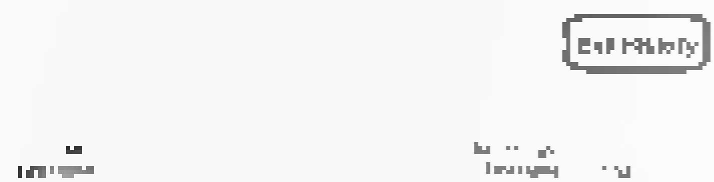
Document numbers will now appear in the box on the right hand of the screen.

E123456
0987896
1098765

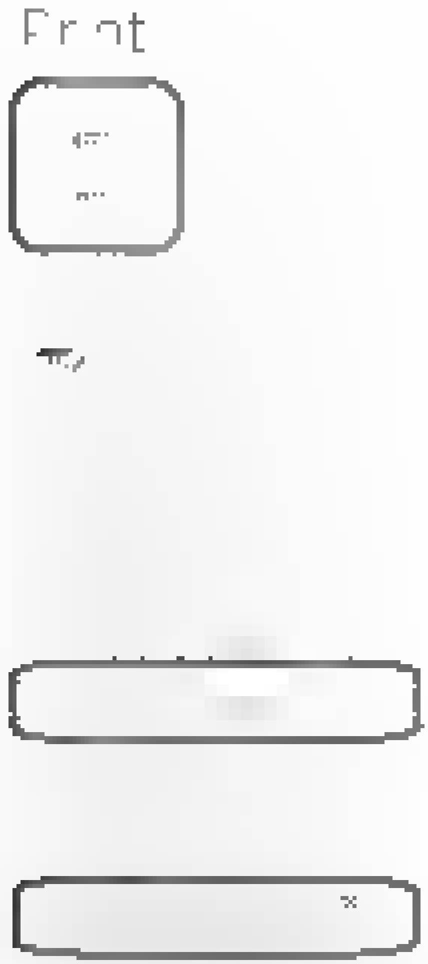
Next click **Finish** at the bottom of your screen. This will create your report. You will now have the chance to verify the information that you have keyed. Once you verified the information, press the button with the globe on the top right. Then select **View in Excel Options**, then **View in Excel 2007 Format**. Once the pop up shows up, press **Open**.



Now that your report is in Excel. Click on the title **Traveller History** and modify the title name to **Exit History**.



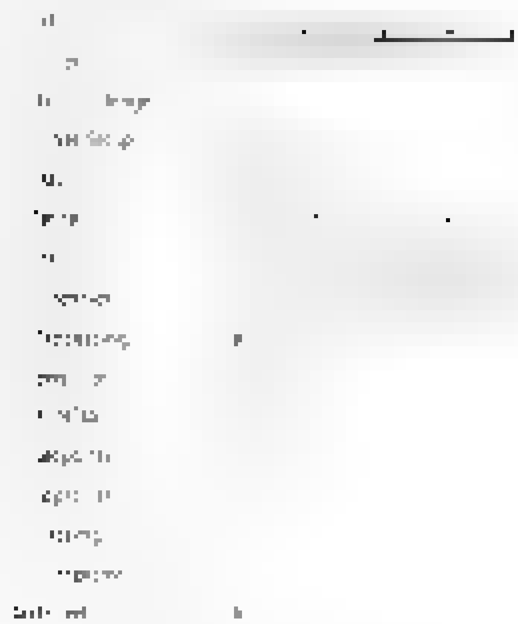
Once this step is complete, your report is ready to be imported into Redaction. When printing the report, change the settings to **Landscape Orientation**, and the scaling to **Fit All Columns on One Page**. Once you have made the necessary changes, press **Print**. For additional information on the importing process, refer yourself to Print to Redaction.



If you need to go back to do another exit report, there is an arrow on the top right of the screen. Pressing this arrow will bring you back to the beginning.

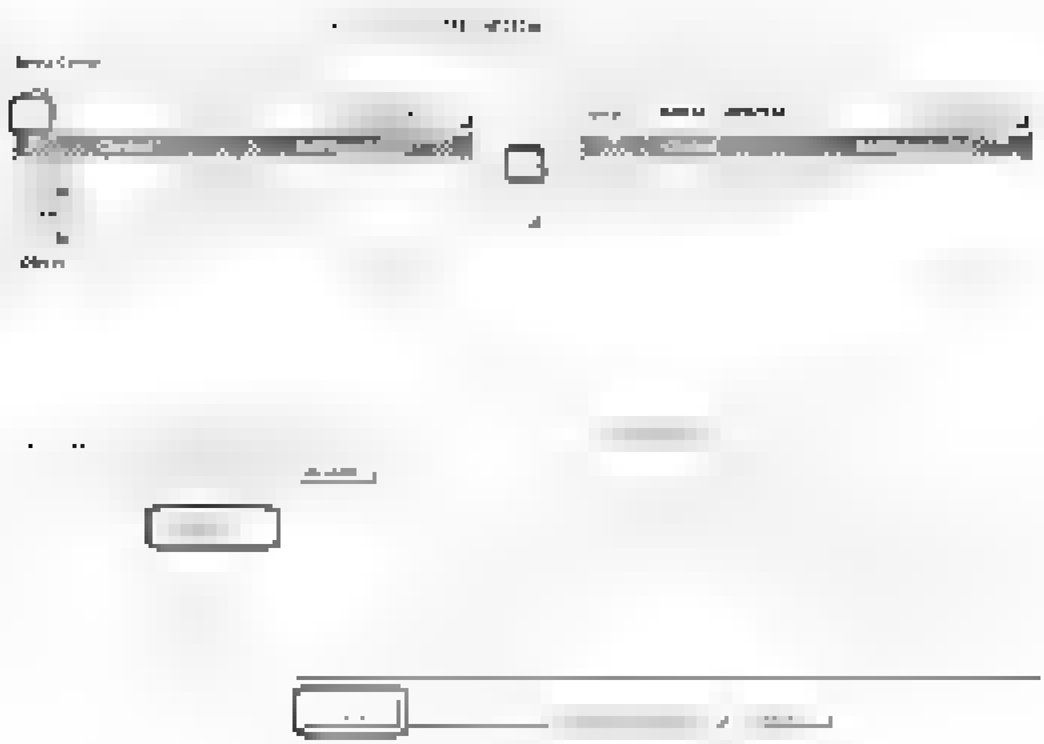
Canada

When performing Exit searches, it must be reflected in APCM. You will need to add the Retrieval action. SYSTEM NOTES (#):



In the **SYSTEM NOTES Name** field, type in 'c' and press **Search**. Select **EXIT** and press > to bring the selection to the right hand side. Type "TR done", todays date and your initials in the **Comment:** field. Put today's date in Date Completed and press **Save**.

If no Exits were found during your search, type "NIL" in the **Comment:** field. Put today's date in Date Completed and press **Save**.



13.1.4 Reviewing Travel History Records

REVIEW

If records were found during your search, the next step is to organize and review the records that were printed into Redaction. Printing to Redaction, stacking and labeling explains how to organize your records in redaction and Annex C: stacking and labeling shows our standard naming conventions.

For the review, you will go through each and every page. The first page of your TH report is always releasable, however you will need to verify that the date range matches the one asked in the request.

ICES TRAVELLER HISTORY – API TRAVELLER PASSAGE REPORT
DATE RANGE

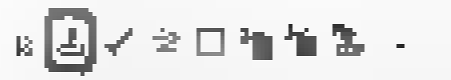
Once you have reviewed this page, right click and select **Release**.

- Selection Pointer
- Color Highlight
- Redact1
- Redact2
- Redact Freehand
- Color Border
- Act Stamp
- Default Stamp
- User Defined Stamp
- Comments/Recommendations
- Consult
- Duplicate
- Not Relevant
- Partial
- Public Granted
- Release
- Withheld

For the second page, which should display all of the entries, you must ensure that all entries are related to correct individual. If there are any entries that have a blank date of birth, or don't correspond to the individual, you will need to sever it. To do this you will want to select the **Scissors** icon at the top of your screen that is with the blue box.

With the scissors selected, highlight the entries that do not belong to your individual. The severing will appear as a pink box on the page.

Next, click on the **Stamp** button.

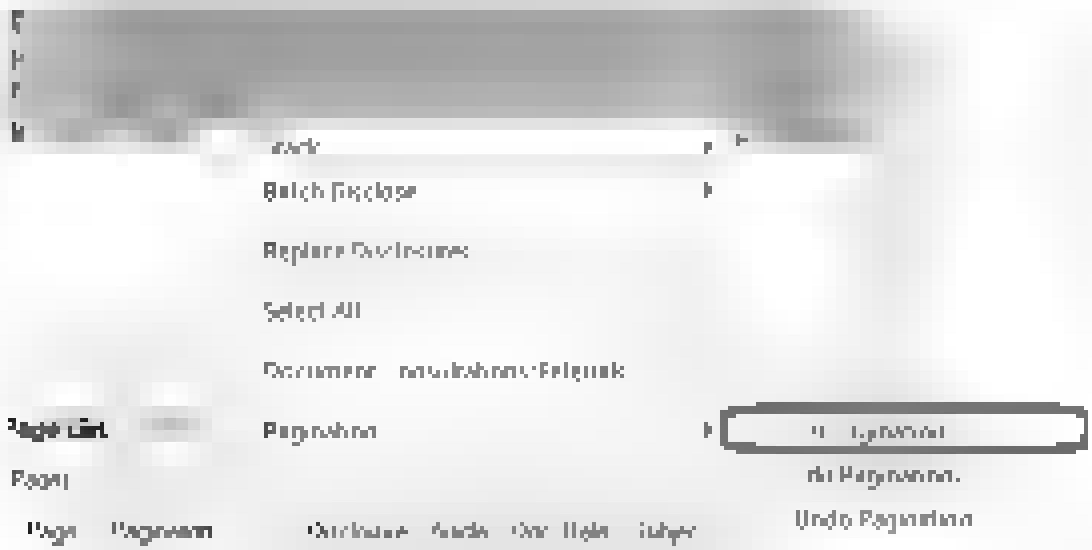


Act Stamp

This will create a pop-up with a list of the sections of the Act. You will need to select what section of the Act you are removing this material under. For TH requests, the information redacted is usually related to another individual. When redacting personal information, we apply sections [illegible] for Access to Information requests, or 26 for Privacy requests. Once you have selected the section appropriate to the request, click Stamp.

Now will stamp section selected by clicking anywhere on the page. Try not to click area with text that your Team Leader will need to review. This stamping action will automatically change the disclosure of your page to Partial. This will be displayed on the left hand side of your screen.

Once you have finished reviewing the records, select all of the reviewed pages (by either holding down **SHIFT** or **CTRL**). Right click on the selected pages, select **Pagination** and then click on **Set Pagination**. This will paginate the pages reviewed. Don't include any ADMIN pages in your pagination and make sure that if your request includes Exits, that they fall after the Travel History Report (ePIMS) in your pagination.



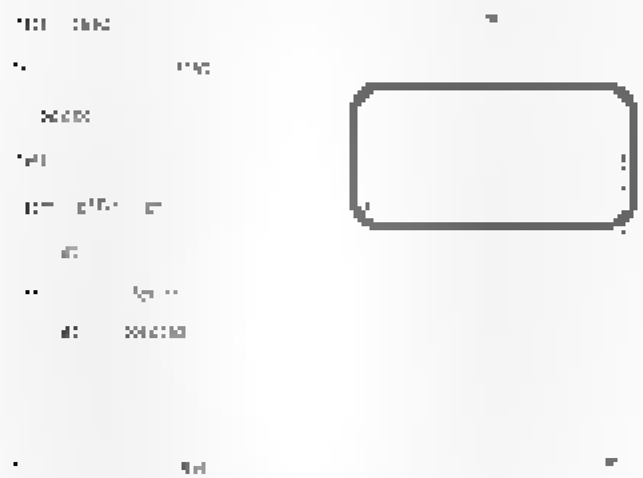
Now you will want to return to APCM, but before you create your Traveller History response letter, verify your Edit Screen and complete the Closing Screen.

First press the Edit button in APCM.

In the Edit screen, ensure that the Officer assigned is yourself, and that the Decision maker is your Team Leader (or the person who will approve the request). Once the verifications are done click **Close**.

To complete your closing screen, in APCM first press the **Close** button.

Once the close screen opens, fill out the **Disposition**, **Method of Access** and **Method of Delivery** fields.



The Disposition is as follows:

- For reports released completely select **All disclosed**
- For reports with redactions on it select **Disclosed in part**
- For a request with <u>no results</u>, select **Does not exist**

For Method of Access:

- For the majority of reports the selection will be **Copies given Paper**
- If the requester has asked for their report electronically, or the pages exceed 50 pages select **Copies given Electronic**
- For a request with <u>no results</u>, select **Not Applicable**

For Method of Delivery:

- For the majority of reports the selection will be **Regular Mail**
- If the requester has asked for the report to be sent via Email, and it is possible to encrypt it through WinZip, select **Email** as the Method of Delivery
- If the requester has sent a return envelope for the report to be sent courier via their own account select **Registered Mail**
- For a request with <u>no results</u>, select **Not Applicable**

Once these fields have been filled out, press the **Add** button located on the bottom of the screen.

Complete all fields in this screen

The **Disposition**, **Method of Delivery** and **Method of Access** will always the same as your previous screen

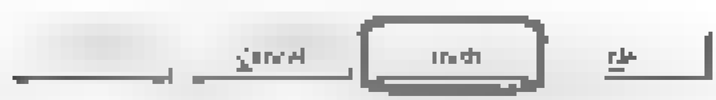
Pages Reviewed, **Released** and **Not Released** can be located in the PROCESSED area of your previous screen

For Translation select **Not Applicable**.

The **Release Date** is today's date

And for version, you will want to select **Complete**

Lastly, select **Finish** when complete



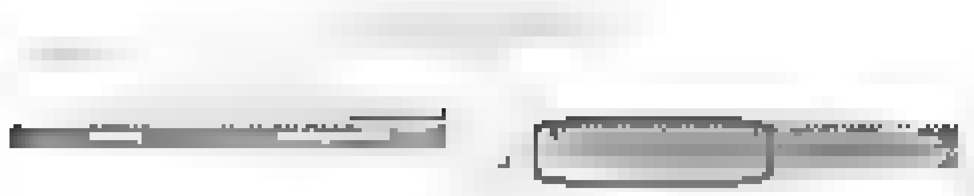
You will now see the newly inputted disclosure on your Close Request screen

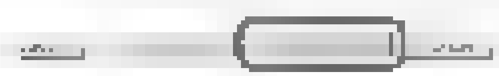
13.1.6 Responding to a Travel History Request

RESPONSE Traveller History

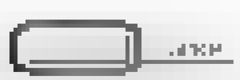
In your APCM screen, go to Add Action, select K – Response and then click on **RESPONSE Traveller History**

In the **RESPONSE Traveller History** box, click on **Requester**. Enter **Date Completed** as today's date, and then press **Save and Letter**. This will generate a letter





When the pop up box appears, choose the template NEW Response – Letter and press Select.



When the letter opens, please amend / verify the following:

First Page:

- Ensure that the address is correct, and that its components are in the correct order:
  - Full name
  - Street address, Apt #
  - City, Province (QC) postal code

[REMOVE "CANADA" at the end of address]

Ensure that Mr. or Ms. is before the last name. If you are unsure of their gender, write their full name instead.

- ie. Dear Mr. / Ms. Smith
- ie. Dear Ashley Smith

Verify that the correct Team Leader's name (that will be approving your review) appears above enclosure

<u>Second Page.</u>

Request Summary:

Remove the privacy brackets and remove any travel document numbers, so that the request text now resembles:

Request Dispositions

If the disposition is "All disclosed" or "Does not exist" remove the sentence starting with "The following line indicates which section(s)..." and the statement "Summary of the Exemptions" in their entirety.

If the disposition is "Disclosed in Part" modify the line "The following line indicates which section(s)..." by dropping the (s) or removing the (), and removing on of the following "was" or "were". Also make sure that all exemptions are included in the Summary of the Exemptions.

Link to Access or Privacy Act:

Only keep the relevant link based on the type of request (Access or Privacy request) and delete the other one.

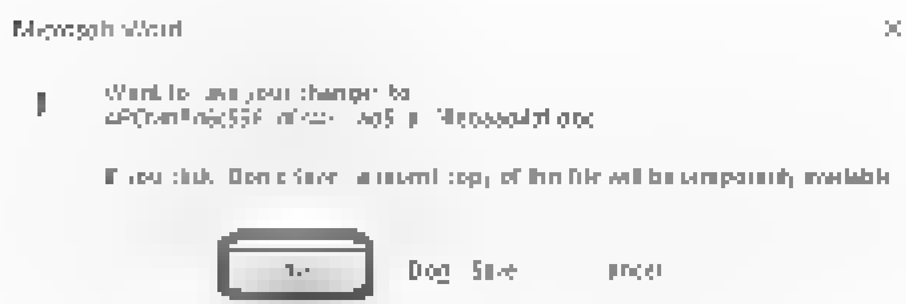
Comments

Keep or remove lines based on the results of the report.

- No – exit report, keep bolded line
- Yes – exit report, delete bolded line

Once all of the changes to the letter are completed, click on File, then Print. Make sure to change your default printer to Adobe PDF and then press Print. Save the letter to a temporary folder.

Then you are done with your letter, close it and you will be prompted to save; press Save



Next an Enter Attachment box will appear, type 'letter' in Description, and then press Attach.

The attachment pertaining to your RESPONSE action will appear in APCM. To access or edit it, click on the RESPONSE line in APCM and press the **Attachment** button above.

13.1.6 Exporting your Travel History Reports

EXPORT/PRINT

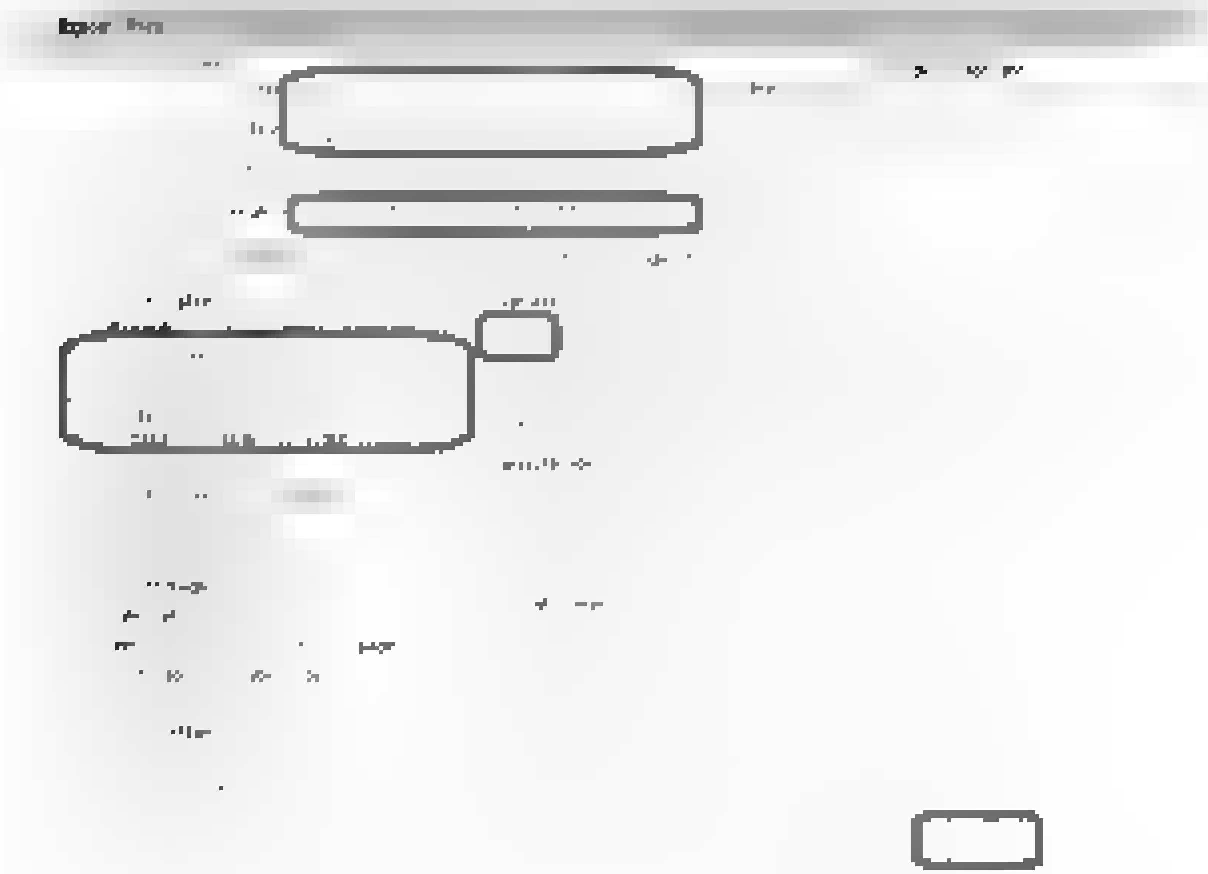
Go back into Redaction and export your Travel History reports to the *temporary folder*.

To do this, click on the **Request** tab in Redaction and then **Export** – **Print**.

Fill out the following fields to

- **Type:** PDF format
- **From:** Request
- **Save location:** *your temporary folder*
- **Preset option:** Release Package
- **Show redaction as:** white
- **Pagination:** Off

Once the fields are filled out, click on **Export**.



Both your response letter and release package are now saved to your *temporary folder*. Go into the folder and select both documents by holding the CTRL key. Right click and select **Combine Files in Acrobat**.

The **Combine Files** window will open. In this window, you can edit the order of the pages should you need to. Make sure that your response letter is the first document in the box, followed by your Travel History reports, and then [illegible] (if any). Press **Combine Files**.

The new PDF with the files combined will now pop up. Once this is done, you can save the file in your respective Team Leader's H folder for Approval. It can be found here:

Once it is reviewed, approved and signed, the Team Leader will then move it into the Mail-Out folder.

13.2 Privacy and Access to Information Requests (not True Access)

The following are all types of Privacy and Access to Information requests common to our office.

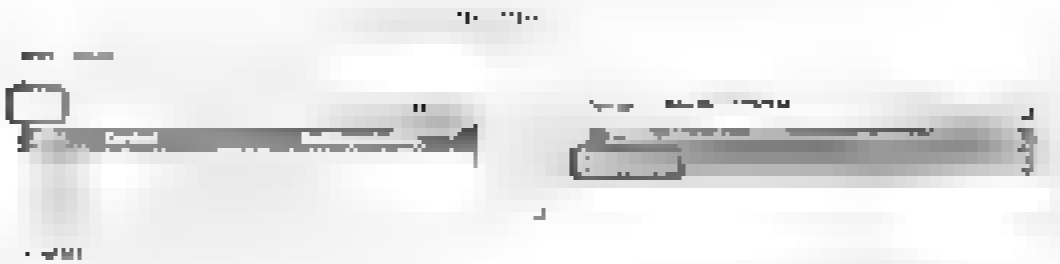
13.2.1 GCMS or FOSS Notes

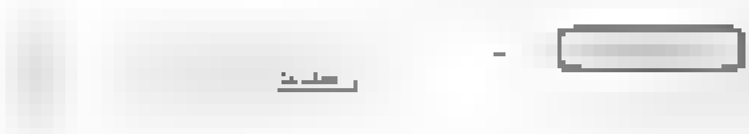
Clients requesting a copy of their GCMS and/or FOSS notes. These requests are done in-house by our Administrative Team, as the ATIP Division has access to these records. FOSS is an obsolete database that GCMS has since replaced. If they are asking for only FOSS records, we still provide them with FOSS and GCMS. For more information on how the GCMS and FOSS records are pulled, see chapters Retrieving GCMS Records and Retrieving FOSS Records.

SYSTEM NOTES

If it's clear that the requester is looking for GCMS and/or FOSS notes, open an action in APCM, selecting "E – Retrieval" and then select **SYSTEM NOTES (a)**.

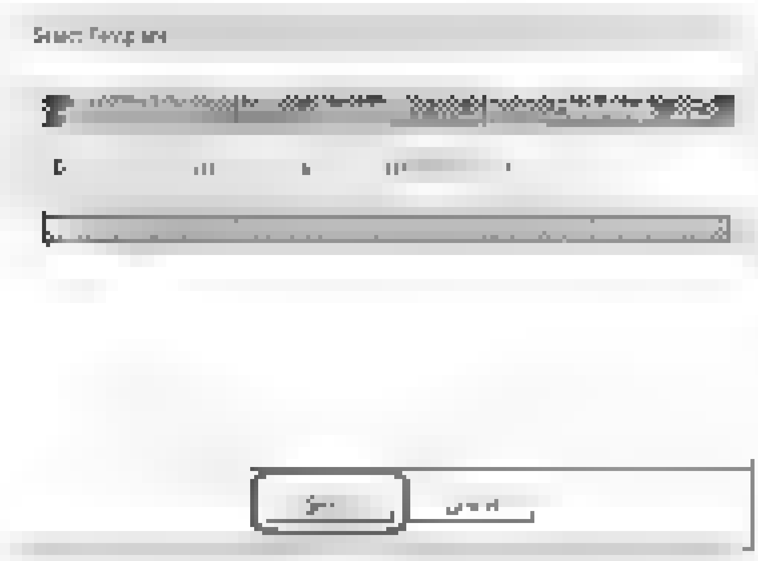
After selecting **SYSTEM NOTES (e)**: a window will open, type "e-" in the Name field and press **Search**. This will show the various options of system notes available. Select the type of request and press [illegible] in order to bring your selection to the right hand side as below. Also record in the Comments field, the date requested and your initials. The **Date Completed** will remain blank, until the action is completed. Now press **Save**.





Once you saved your retrieval action, you will generate an email to be sent to the ... team to request the retrieval of these records. To do this, select the **SYSTEM NOTES** line for GCMS in APCM and then press Email. **If you are asking for both, you will need to do this step again.

You will now be given 4 options of the email template. Select what is applicable (**GCMS Request** and/or **FOSS Request**) and press Select.



An email will populate and you can review the email for completeness and accuracy, and then press **Send** once complete.

Some key points when reviewing your email:

- Ensure that the UCI is included in the email. It is always good practice to make the UCI more visible (increase the font, change the colour to red, etc.)
- If a UCI contains 10 digits, no FOSS information will exist for that UCI
- If a specific application is sought by the requester, make sure it is mentioned in the email
- Make sure to remove the privacy brackets out of the text
- Always make sure that your email is encrypted before sending the email

The clerical team is given working days to input your records directly into Redaction. Once the action is complete, they will send you an email.

13.2.2 Immigration Records

Clients seeking copies of records held by the Canada Border Services Agency (CBSA) relating to their immigration matters. This request usually involves tasking Liaison Officers (LOs) in the Intelligence and Enforcement Branch and possibly other region(s). Included in our response is also a copy of the client's GCMS notes and FOSS notes (if any exist).

It is also important to run a Full Travel History to include in your records. A Full Travel History will also show any referrals and seizures that have occurred, and it's likely that Port Office holds some records on the client as well, so they will need to be tasked. An Exit Report should also be provided to the applicant.

An Analyst can also use NCMS to determine which region may hold records in relation to the Immigration file being sought. NCMS is also a helpful tool to help with your review, when determining what investigations/actions are ongoing or concluded.

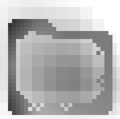
The first step is to find out where the Immigration file is located. To do this use NCMS.

13.2.2.1 NCMS

To log into NCMS, follow the RCT log in screen located here:

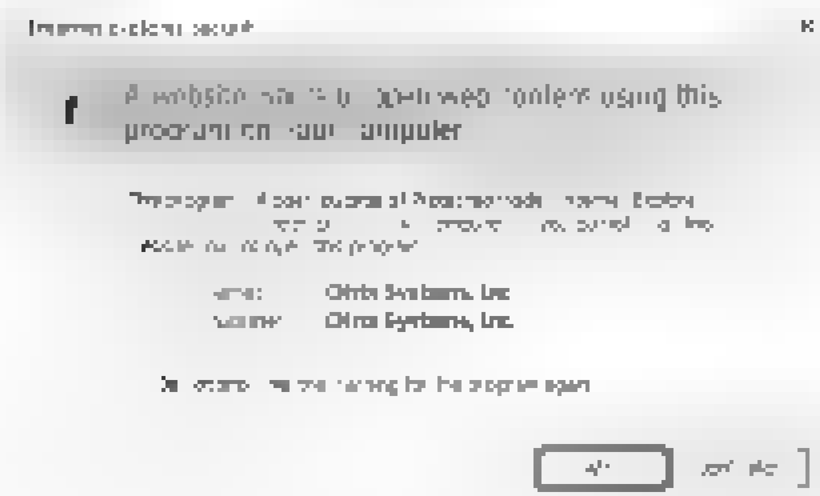
To log into Citrix, use you Citrix ID along with the password associated with your Citrix account.

Once the IHCC page opens up you will see 4 folders, click on the NCMS folder.



Next, click on the NCMS-SNGC Prod icon.

An Internet Explorer security pop up may appear. Press Allow



A Citrix Receiver – Security Warning may also pop up. Press Permit use

The NCMS login screen will now open

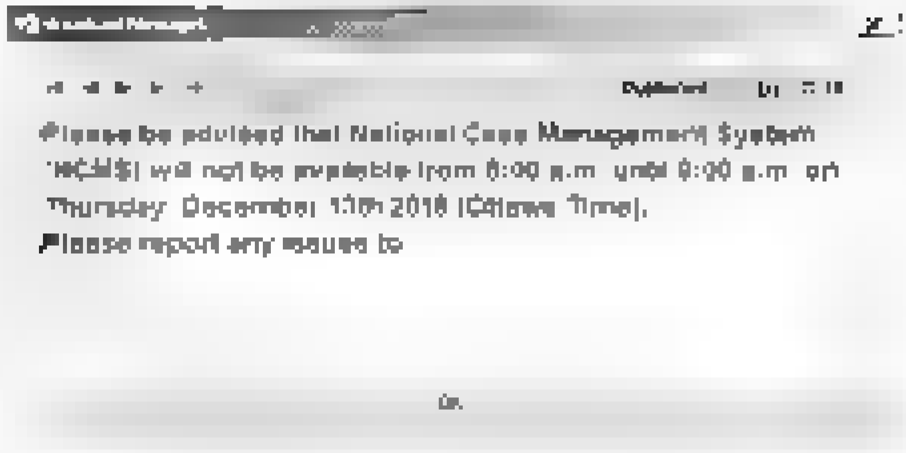
Access to NCMS

A completed User Request Form for IRCC Systems – OGD (IMM 5600 E) (PDF, 4 MB) form should be submitted to your Access and Security Coordinator (ASC).

All new users to IRCC systems must also complete and submit an Electronic Network Access and User Agreement ([illegible] – PDF, 19 KB) form.

NCMS Roles: After you have been granted access to NCMS, your supervisor or NCMS Regional Coordinator must assign a user role to your profile before you can start using NCMS. CBSA NHQ users may contact the NCMS mailbox for role assignment.

At times, Broadcast Messages will appear. If one does, press OK.

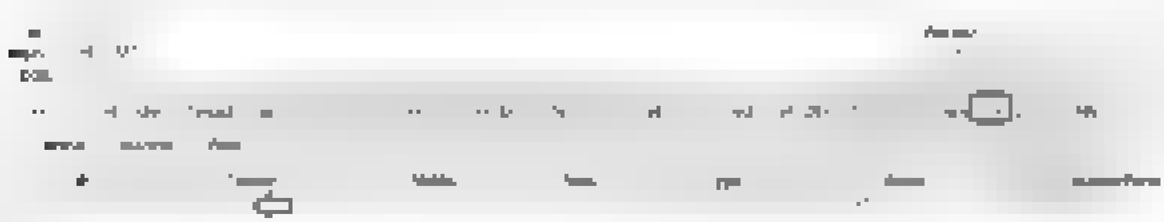


Once in NCMS, press **Retrieve** at the bottom of your screen.

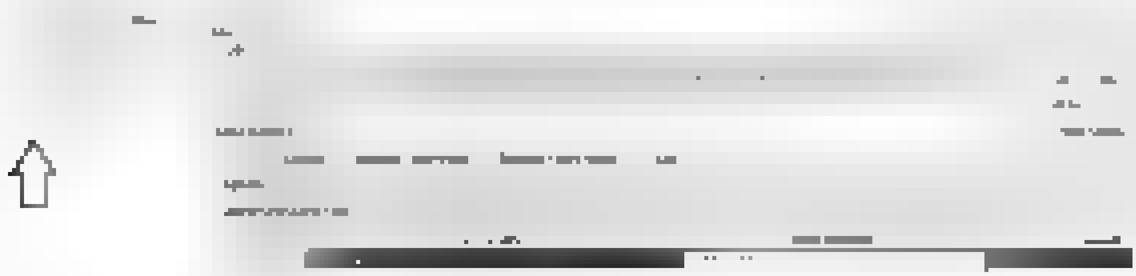
A Retrieve Single Client box will pop up. Enter your UCI / Client ID and press **OK**.

Once on the Client screen, press the **File** tab. The holder of the file should be listed there. It is important to note that you will not task for NCMS files if the Holder of the file is not a CBSA office.

The Status column may give more information as well on whether or not the file is active. If the file has been destroyed, then you will not need to task that region for the NCMS file.



The column on the left on your client's main screen also gives information as to what is going on with the client file. You may see enforcement actions, investigations, court information to name a few.



You may expand any of these actions, by pressing + to obtain additional information pertaining to the client's immigration file. If an investigation is concluded, it should allow for more information to be released under the Act. Whereas, if there was an ongoing investigation, you will need to protect information related to that investigation. This section of NCMS can be very useful when reviewing your file.

13.2.2.2 Adding your System Notes in APCM

SYSTEM NOTES

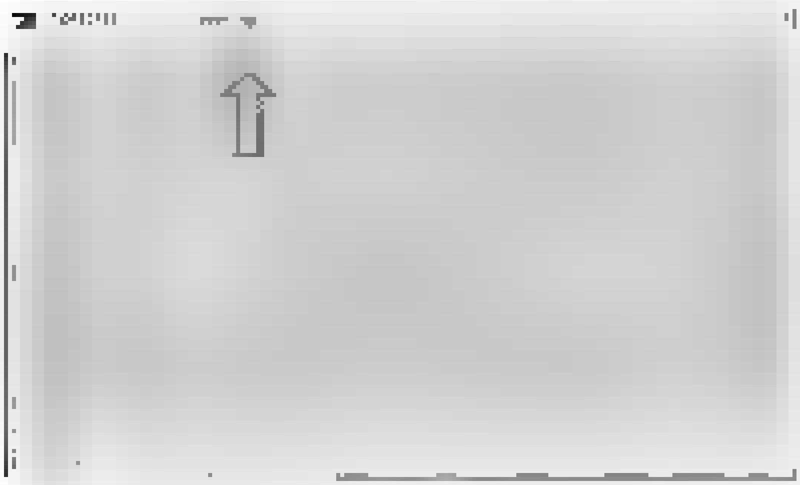
Task the administrative team for GCMS and FOSS notes. The steps in tasking GCMS and FOSS notes are same as mentioned in GCMS or FOSS Notes. If the UCI contains 10 digits, no FOSS information will exist for that UCI.

Next, generate a full Travel History Report for your file. A full Travel History consists of the same steps as explained in Running a TH Report with one difference. When on the ICES Reporting Screen, you will choose the option **Traveller Passage Report** instead of **ATIP Travel Passage Report** (in the Traveller History drop down). This report will display three additional columns, one of which is the referral type.

Referral types marked as are indicators that the client crossed the border without being referred to secondary. Since the client crossed without any referral the region won't have any records pertaining to that entry. Any other referral type indicate that the client was referred to secondary when entering Canada, and it is possible that region holds records related to those entries.

Once you run the new TH report, print your full TH report to Redaction.

Run an Exit Report as well, and print your Exit Report to Redaction.



Don't forget to add the Actions related to the GCMS, FOSS, NCMS, TH and Exits to your file in APCM.

RETRIEVALnotice

Task the region(s) that holds the immigration file (as shown in NCMS). Additionally task any region(s) where secondary referrals were present in the full Travel History Report (if any were present). Be sure to include a screen clipping of the NCMS screen, as well as any entries found in the TH, in your RETRIEVALnotice email when tasking the region(s).

To perform an information retrieval, follow the steps found in the chapter Sending Retrieval.

REVIEW

The review of a Privacy or Access to Information request is same as the review of any type of file, the steps being: stack, index, highlight recommendations, and then redact. The only thing that we don't usually do is highlight recommendations.

related to personal information on these files. Focus on highlighting the OPI recommendations related to their areas of expertise.

The chapter Reviewing Records provides further explanation on the Review Stage.

RESPONSE

Prior to submitting your file for approval, you will prepare your response letter. The chapter Preparing Your Response Letter provides instructions on how to create your letter.

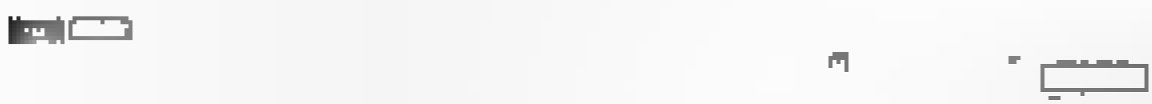
RESPONSEadditionalinfo

There may be instances where additional records are received after you have already sent a response. Instructions can be found in the same chapter: Preparing Your Response Letter.

13.2.3 Grievance or HR Files

Employees wishing to have a copy of their grievance or HR file. The Analyst will task the region that the client is located in, as well as the Human Resources Branch at Headquarters (HQ).

If it is not already indicated in the request, you may look in the Outlook address book (located under the Home tab) to find out what region they are located in.



If it is still not clear where their place of employment is, you may place this file on hold by doing an ACK-complete.

RETRIEVALnotice

Task the area that holds the Grievance File (the region they belong too, or HRB at HQ if they are a headquarters employee). If they are regional, always task headquarters as well, the grievance may have escalated to HQ.

To perform an information retrieval, follow the steps found in the chapter Sending Retrievals.

REVIEW

To review a Privacy or Access to Information request is like the review of any type of file, the steps being: stack, index, highlight recommendations, and then redact. The only thing we don't usually do is highlight recommendations related to personal information on these files. Focus on highlighting the OPI recommendations related to their areas of expertise instead.

The chapter Reviewing Records, provides further explanation on the Review Stage.

RESPONSE

Prior to submitting your file for approval, you will want to prepare your response letter. The chapter Preparing Your Response Letter, provides instructions on how to create the letter.

13.2.4 Any and all Emails held by the Following People about Me

Clients wishing to have emails where they are mentioned, should include a list of people who may hold the emails they are looking for.

RETRIEVAL notice

The LO of the area(s) in which the mentioned people are employed, are tasked by the ATIP Analyst. The LO's are to task each individual mentioned in the request directly to their personal work account. If you are tasking multiple LO's only send them the names of those people in their region/branch.

It is important, when sending out the tasking, to ensure the anonymity of the requester. Replace any wording indicating the identity of the requester (all emails pertaining to myself) with the 3rd person (all emails mentioning John Smith).

If there are multiple people to contact, individual emails are to be sent to each person separately by the LO; they are not to include the names of the other people being tasked for the request. IT/Security are rarely contacted to extract the information directly from a server, with the exception that the individual has recently left the agency, retired, or is on an extended leave of absence.
Note: The client should be made aware that the person they are seeking the information from will be contacted to provide the documents in question.

additional records that were missed (if any exist)

REVIEW

The review of a Privacy or Access to Information request is same as the review of any type of file, the steps being: search, index, highlight recommendations, and then redact. The only thing that we don't usually do is highlight recommendations related to personal information on these files. Focus on highlighting the OPI recommendations related to their areas of expertise.

The chapter Reviewing Records provides further explanation on the Review Stage.

RESPONSE

Prior to submitting your file for approval, you will want to prepare your response letter. The chapter Preparing Your Response Letter provides instructions on how to create your letter.

RESPONSEadditionalinfo

There may be instances where additional records are received after you have already sent a response. Instructions can be found in the same chapter, Preparing Your Response Letter.

13.3 Access to Information Requests (True Access)

The following are types of Access to Information (True Access) requests common to our office.

Information about Canada Border Services Agency seizures on contraband substances
Requesters seeking information about the workings of the CBSA. When requests are too broad, the ATIP Division will contact the client to see if we can narrow down their request to limit to time frames, locations, and specific items. From there, the Analyst will task the appropriate areas, whether that is only a specific region, HQ, or a combination of the two.

Briefing Notes/Materials – Requesters seeking information about the workings of the CBSA. They usually request these based on who they are from, or concerning a certain topic. When requests are too broad, the ATIP Division will contact the requester to see if we can narrow down their request and limit it by time frames, locations, and/or specific items. It is good practice to suggest to the client to re-scope their request to a list of these items, and then making a second request for the specific documents (once they receive the list). It is also highly recommended to suggest to the client to exclude those items that would be considered a cabinet confidence in order to expedite their request.

Statistics – Requesters seeking information about the workings of the CBSA. Common statistic requests pertain to seizures and immigration statistics. When a timeframe is too broad, it is recommended to suggest a narrower scope.

Emails held by Senior Officials – Requesters seeking information usually related to specific topics, seeking an inside perspective of the dealings of the CBSA. When requests are too broad, the ATIP Division will contact the requester to see if we can narrow down the request and limit it by time frames, locations, and/or topics. We do have a frequent requester who submits this type of request. His requests are handled a little differently. See Email In-box Requests.

For True Access, the steps are the same as any other request, with just a few additional steps added.

RETRIEVAL notice

Task the areas who hold the specific information being sought. If you are unsure of who to task, refer to similar requests submitted in the past and see who were tasked. A search on our intranet can also help narrow down who would be in possession of the information requested. Giving an LO a quick phone call is also helpful if you are unsure.

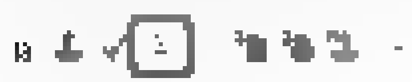
Once you know who to task, follow the steps for it in the chapter Sending Retrievals.

When records are received from the OPI, it is mandatory to record the OPI's recommendations into Redaction.

13.3.1 Recording Recommendations of the OPI

Due to their expertise in the information, OPIs review and provide recommendations on the records they have submitted. There is no need for OPIs to identify specific provisions of the Act as a basis to redact certain information as ATIP will do so. However, in order for the proper exemption to be applied, the OPI must advise ATIP of any adverse implications and provide rationale for any recommendations provided.

Prior to reviewing the records, it is important to highlight, in yellow highlighter, any recommendations submitted by the OPI into redaction. To do this, select the highlighter icon at the top of your screen in redaction and highlight the areas that are recommended to be exempted. If an entire page is to be withheld, a highlighted line down the entire page is sufficient. For consistency within the division, always start with YELLOW highlight for OPI recommendations.



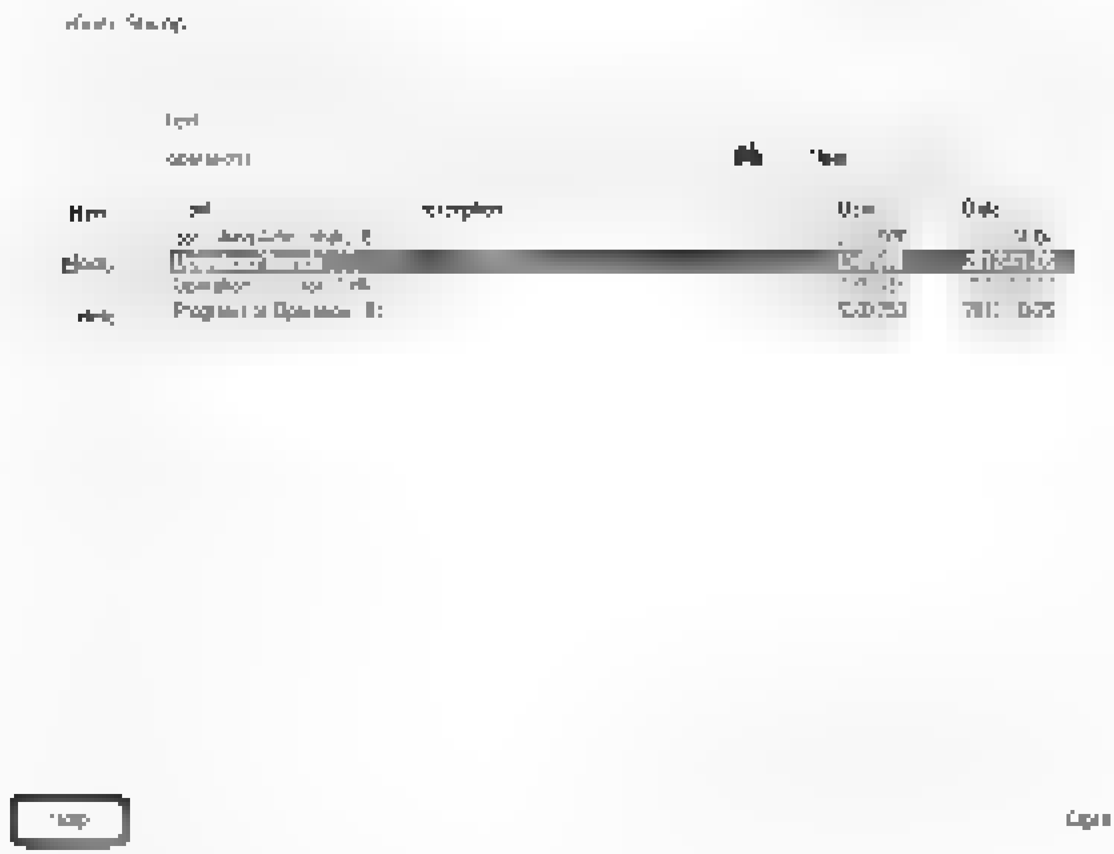
Using the document index to add notes is helpful when your Team Leader is reviewing the file. Adding remarks are especially helpful in the case where more than one recommendation are on the page (ie. if you have also consulted with another area for recommendations). To record remarks, press the icon at the bottom right of the Redaction screen. This opens the Document Index area. Select the **Notes** tab, and the press the **Document** button. The area will turn white and you will be able to edit the text. Press **Stamp** to place the date and your user ID and then type in your comments. Press **Save** when you are finished with your comments.

If you have several recommendations from different OPIs, you may colour code your highlights. It is important to note which highlight belongs to what OPI, either with a custom stamp, or the document index.

To create a custom stamp, select the **User Defined Stamp** in Redaction.

First, search for a previously created stamps. To do this, type in the text that you are seeking (or a portion of the text) and press the binoculars to perform the search.

If you find what you are looking for, click on it and press **Stamp**.



If the stamp isn't there, create your own by clicking on **New**.

Type the name of the New Stamp in the textbox and press **Save Close** when complete.

Select User Defined Stamp again in Redaction and search for your newly created stamp. Once found, select and press **Stamp** to use it. You may use these custom stamps to stamp any text that you feel will help a reviewer navigate through your file.

13.3.2 Reviewing True Access Files

REVIEW

The review of a True Access request is the same as the review of any type of file, the steps being, stack, index, highlight recommendations, and then redact. However, True Access files cannot be closed until an agreement is reached on all recommendations provided by the OPIs. As an Analyst, you may propose to sever more information. If the OPI has asked that something be exempt and you disagree, you need to work with the OPI and come to an agreement of what will be redacted.

The chapter Reviewing Records provides further explanation on the Review Stage.

13.3.3 Agree – Disagree / Resolving Recommendations

Once you have completed your review, any disagreements that you may have with the recommendations received will need to be resolved before proceeding with your file. If you have any uncertainty on your own stance, this is a great time to sit and discuss with your Team Leader (or whoever will approve your file).

<u>The following actions are mandatory flags for all True Access and AC files.</u> These flags indicate whether or not the OPI and Analyst agree, disagree, or if a previous disagreement has been resolved.

Please place the appropriate flag on your file prior to submitting it for approval. The flags can be added by going to **Add Action** in APCM, and selecting **Mandatory** and the applicable MANDATORY flag.

MANDATORY > Recommendations – AGREE with

__Recommendation-AGREE__

- This flag indicates that you are in full agreement with the OPI and have followed the recommendations fully.

MANDATORY > Recommendations – DISAGREE with

__Recommendation-DISAGREE__

- This flag indicates that you are not in agreement with the OPI and did not follow all of the recommendations provided. When creating this action, input the name(s) of the OPIs which you did not come to an agreement with. Make sure to add notes on the pages in question in Redaction. If the TL / Assistant Director (who will approve the file) also disagree with the OPI's recommendations, a copy of the revised disclosures must be sent to the OPI for review. All items must be resolved before you can proceed any further with the file.

MANDATORY > Recommendations – RESOLVED with

- In the instance where there is a disagreement, the **Recommendations – RESOLVED with** flag is to be placed on the file once it is resolved.

13.3.4 Response Letter

RESPONSE

Prior to submitting your file for approval, you will want to prepare your response letter. The chapter Preparing Your Response Letter provides instructions on how to create your letter.

RESPONSE additionalinfo

There may be instances as well where additional records are sent after you have already sent a response. Instructions can be found in the same chapter Preparing Your Response Letter.

13.3.5 Flags

HEADS-UP Formal (+): LEGAL (Director Approval)

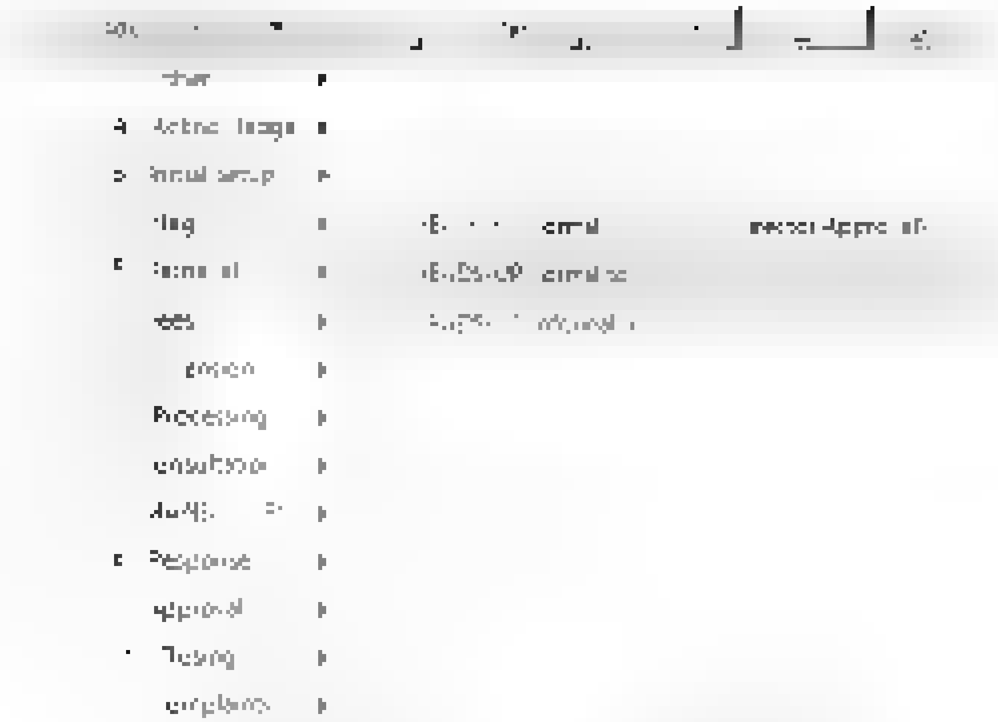
HEADS-UP Formal (0, +)

HEADS-UP Informal to.

A True Access request always has a Briefing Folder and Communications flag. These flags are essential as they give Communications an opportunity to write media lines (if required) before any information on the Agency is released. More information on the Communications Review related this flag can be found in the Approval of Files chapter.

Flags are also valuable reminders and can be added to the file as you work through it.

To add a flag, go to Add Action, Do Flag and you will see Formal and Informal options.



Once the Add Action has popped up, type a + into the Unit/ Organization field, and press **Search** to see the formal flags available

You may also use informal flags if an OPI or SME requests to review the release package before it is disclosed. In these cases, use the name field or Unit/Organization to search them, and press the > to bring them to the right to capture them as the contact for the flag

13.3.6 Uploading onto the Public Safety Portal (True Access Only)

Once the file has been approved by the TL and the Assistant director, upload the release package onto the Public Safety Portal. The chapter Uploading onto the Public Safety Portal gives more in-depth instructions on these steps.

13.4 Email In-box Requests (True Access)

These requests are commonly made by a frequent requester. The applicant is looking for entire email in-boxes, usually the in-boxes of CBSA's senior management. In order to reduce the workload and expedite these requests, the requester has agreed to break these requests into two phases: **Phase 1** and **Phase 2**.

When receiving one of these requests, the first step is to look up in Outlook where the employee is located within the Agency. If you are unable to locate the employee's name in Outlook, do a search in our Intranet. Otherwise, you will need to contact our IT Helpdesk to find out where the individual is located within the Agency.

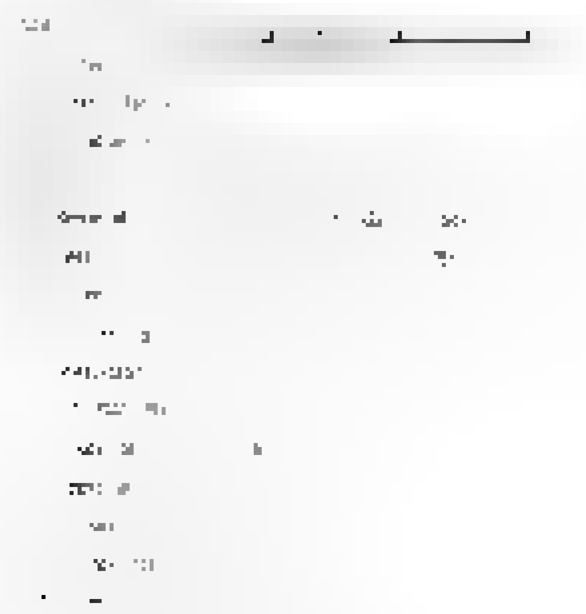
Note: With these specific requests the employee is not to know that they are the subject of the request until after the retrieval is done. The retrieval is done only by ISTB and not the individual.

RETRIEVALnotice

Once you have determined which Branch/Region the employee is located in, you are ready to task ISTB.

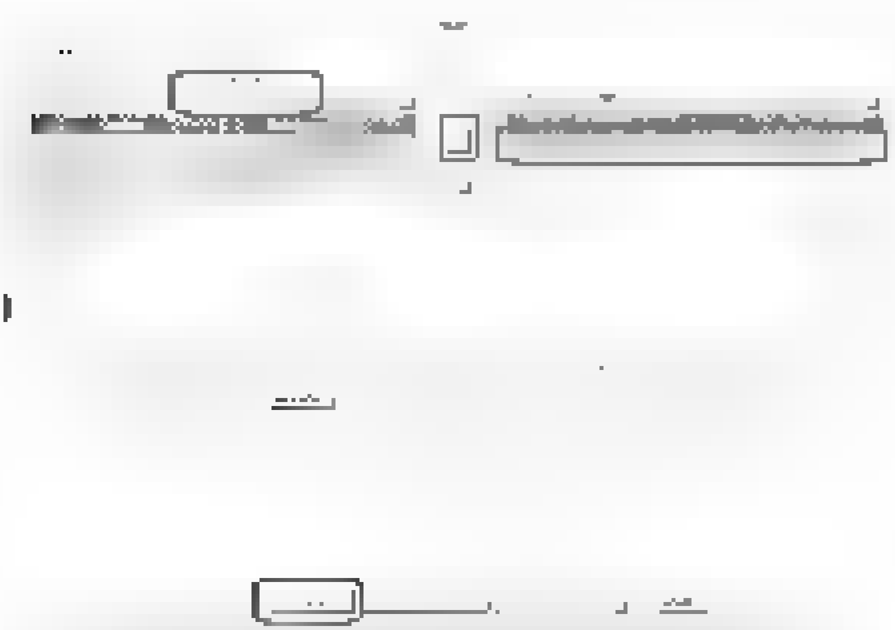
Note: If the employee is not in the Directory or Outlook, you will still have to task to ISTB and wait for them to respond back with a confirmation that the employee is no longer within the Agency. The request will then result in a Nil response to the requester.

The retrieval steps for this type of request are different than those found in the chapter Sending Retrievals. For this type of request go into APOV, go to **Add Action**, **E-Retrieval** and then **RETRIEVALnotice**.



Once the ACTIVITY Assign box pops up, type in "inform" in the Unit/Organization section and press **Search**. You will see the selection ATIP Liaison, Information, Science and Technology Branch. Select, and press > to bring it to the right hand side.

Next, type "Retrieval sent" in the "Comment" field. Don't forget to include today's date and your initials. Leave Date Completed open (blank) until you receive the information, and then press **Save**.



Once you click save, select the retrieval line in APOM and press **Email**.

When prompted to select a template, choose **Phase 1 (M) – R** and press **Select**.

This action will produce the following Retrieval Email. If the request indicates a time range that ends with "to present", be sure to add the date that the request was received (in the example below the request was received on January 1, 2018).

You can also note the location of the subject in the request at the top of your retrieval email. Once your email is ready to go, press **Send**.

Example Email:

__Please note,__ The employee is located in the Northern Ontario Region.
Special instructions are also below.

PROTECTED
OUR FILE / NOTRE REFERENCE: A-2018-12345 / S

Request Text / Texte de la demande

PHASE 1 – We wish to access all emails pertaining to (SMITH, John) for the period of April 1, 2014 to present **(January 1, 2018)**

Hello
[illegible]
Special instructions to IT

1. Please note that the employee is NOT to be advised of this request.
2. Only copy the emails that fall within the time frame requested.
3. The information is to be copied to our drop zone at

****

Note: It is important to **Print to Redaction** all emails (including retrievals) into your **ADMIN file.** You should go into your In box – sent items to print your retrieval email into Redaction.

Organize your admin file (and later any records) by stacking and indexing them. Printing to Redaction, Stacking and Indexing explains how to print to Redaction, set up your printer and organize your items in Redaction. Annex C – Stacking and Indexing shows the various naming conventions used in our group.

Once you receive a notification (usually by email) that ISTB has dropped the information onto the Z: drive, the information will need to be retrieved. It is important not to delay retrieving the mailbox dropped by ISTB to ensure IT has retrieved the correct mailbox.

13.4.1 Retrieving Emails from the Z: Drive

Open Microsoft Outlook and click on the File tab

Once the tab opens, click Open & Export.

Next, click on **Open Outlook Data File**.

Once the Open Outlook Data File box opens, select the Z: drive and double click on the file that you need to transfer to Redaction.

Click on the folder and then click on Open at the bottom right of the box. Click again on the item that just opened and then click OK at the bottom right or double click on the item. The folder will then appear in your Outlook.

13.4.2 Exporting Emails to Excel and to Redaction

From Outlook, click on the **"Developer"** tab located in the menu bar and then on the **"COM Add-ins"**.

A pop up window will open. Uncheck the following Entrust items and click "OK".

Entrust Entelligence Security Provider for Outlook (64-bit)
Entrust Entelligence Security Provider for Outlook (32-bit)

<u>Note</u>: You will need to check these boxes back once you are done the process below.

Next open Redaction for the file in question. You will open the macro Excel spreadsheet Pase1_EmailExtract.xls (keep it on your desktop for easy access). The Excel spreadsheet can be found in the ATIP Division Handbook folder.

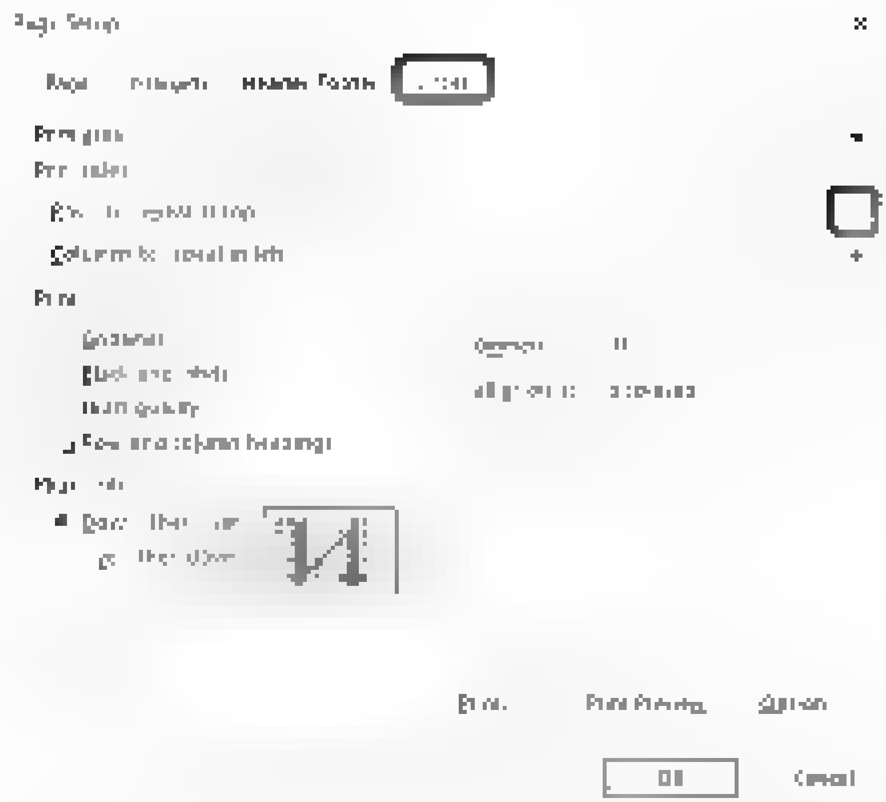
When you first open the macro Excel spreadsheet, a Microsoft Excel Security Notice may pop up. If it does, select **Enable Macros** to proceed.

A pop-up window will open: click on **Continue**. Once the second pop-up window called **Select Folder** opens, select the .pst file that you imported into your inbox and click on **OK**.

Once all emails are all imported to the Excel spreadsheet, you will need to modify the Excel page. In Microsoft Excel, click on the **Page Layout** tab, and then under the **Scale to Fit** section, click on the little arrow in the right bottom corner.

A pop-up window will open. On the **Page** tab, under the "Scaling" item, modify the "**Adjust to**" to "99%" normal size, then checkmark "**Fit to**" and change the range to "1" page(s) wide by "200" tall.

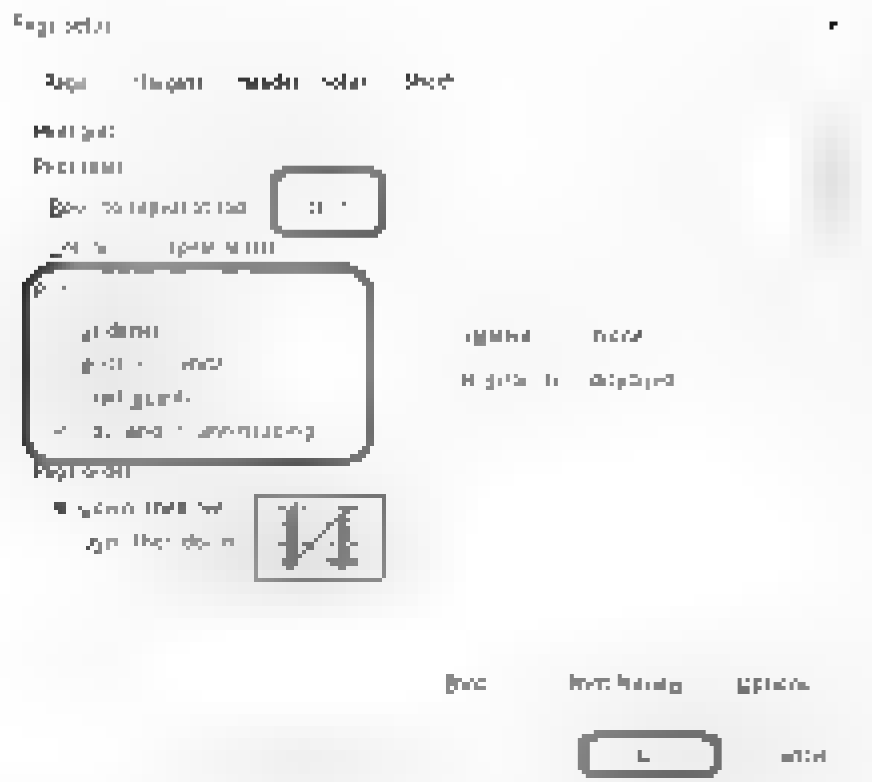
In the same window, under the **Sheet** tab, click on icon on the right hand side of "**Rows to repeat at top**".



The window will then shrink

Select 'Line 1' in the far left corner of the Excel sheet that contains the menu [illegible] form. Subject [illegible]. Once selected, click on the icon (red/blue) on the right hand side of the small box

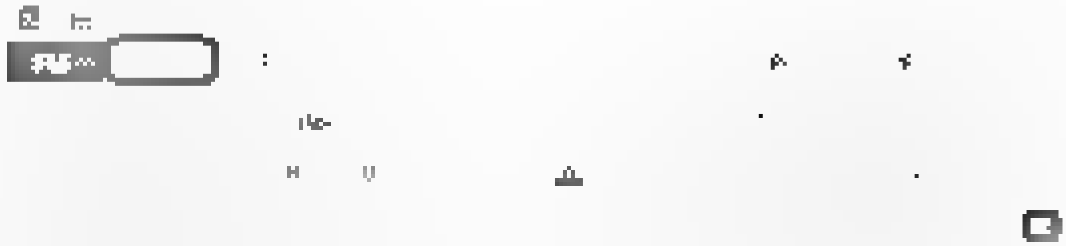
Back on the Sheet tab under the 'Print' item, check the 'Gridlines' and 'Row and column headings' boxes and then click OK



Now click on the **View** tab from the menu bar. Click on **Page Break Preview** and adjust the columns manually to fit the text in them if needed.

Now select the whole text by clicking on the left corner of the sheet itself.

Click on **Home** tab, then click on **Alignment** little arrow on right corner (in light grey).



A pop up window will now appear. Under the Alignment tab, in the Vertical box, select the Bottom option. Then click OK.

The Excel spreadsheet is now ready to be printed to Redaction. For additional information on the importing process, refer yourself to Print to Redaction.

ectly in the C: Drive. In the specified folder, please save your spreadsheet as "Emails sorted A-2018-XXXXX"

13.4.3 Notification of the Individual

When processing requests for employee email accounts, please make sure to inform the employee in question that a request has been received for their emails. This notification should be done once the email account has been retrieved and is saved to our J-drive.

You will also need to offer the employee a copy of the proposed disclosure prior to release. This applies to both Phase 1 and Phase 2 requests.

Example of an email to send:

Good morning,

The ATI Privacy Division has received an Access to Information Act (the Act) request for all your emails, including attachments, since February 1, 2016.

In an attempt to reduce the number of records to be reviewed, the requester is first seeking the subject headers of all emails in all folders. Once the available information is sent to the requester, emails of interest will be selected for their content (including all attachments). Your assistance will be required to go over the selected emails in order to identify any sensitivity with the information being requested. Please note that the requester is not seeking anyone's personal information.

To protect the integrity of the request process, the ATI-Privacy Division has saved a copy of your email account. You may therefore proceed to work in your MS Outlook account as usual.

As employees of the Canada Border Services Agency (CBSA), you have an important role to play in ensuring that ATI-Privacy legislation and its associated principles, standards and obligations are upheld. I know I can count on your full support in ensuring that CBSA complies fully with the requirements of the Act.

Bonjour,

La Division de l'AIPRP a reçu une demande en vertu de la Loi sur l'accès à l'information (la Loi) concernant tous vos courriels envoyés ou reçus depuis le 1er février 2016, y compris les pièces jointes.

Afin de réduire le nombre de courriels devant être examinés, le demandeur sollicite d'abord les titres des courriels de chaque fichier. Une fois que les titres disponibles lui sont envoyés, les courriels d'intérêt sont sélectionnés selon leur contenu (y compris toutes les pièces jointes). À ce moment-là, vous devrez aider à vérifier les courriels sélectionnés en vue de déterminer si, parmi les renseignements qui font l'objet de la

recherche, il y a des renseignements de nature délicate. Veuillez noter que le demandeur ne sollicite pas de renseignements personnels.

Afin de protéger l'intégrité du processus de demande, la Division de l'AIPRP sauvegarde une copie de votre compte de courriel, ce qui vous permet d'utiliser votre compte Outlook comme d'habitude.

En qualité d'employés de l'Agence des services frontaliers du Canada (ASFC), vous jouez un rôle important pour veiller au respect de la législation sur l'AIPRP ainsi que des principes, des normes et des obligations connexes. Je sais que je peux compter sur votre soutien inconditionné pour s'assurer que l'ASFC satisfait pleinement aux exigences de la loi.

13.4.4 Phase 1 – Review

REVIEW

The review of these types of requests is a bit different than other requests as the response is done in 2 phases.

Although Phase 1 is considered an "Other" type request, we treat them similar to a True Access request. The steps are the following: track, index, highlight recommendations, and then mark for redactions.

The chapter Reviewing Records, provides further explanation on the Review Stage.

In short, Phase 1 involves only the subject headings of the emails retrieved.

For subjects that are unclear, you may have to go back into your inbox and source the email to determine whether or not they are business related. It is important to look out for titles containing personal information. In these instances, you can redact the personal information and release the rest of these titles. Your Phase 1 response will only consist of a list of emails.

Due to their familiarity with the emails, it is important to have the subject of the request review and provide recommendations on the Phase 1 pre-release package.

13.4.5 Response Letter – Phase 1

RESPONSEphase1

Prior to submitting your file for approval, you will want to prepare your response letter. The chapter Preparing Your Response Letter provides instructions on how to create your letter. Phase 1 you will use the regular response letter.

13.4.6 Phase 2 – Review

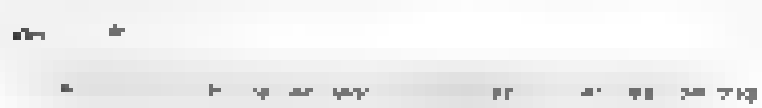
Once the requester responds with their selections, Phase 2 begins. This phase involves printing the selected emails (including their attachments) into Redaction and then reviewing them as you would any other True Access file. After the emails have been imported into Redaction, consultations will then need to be sent, including to the person concerned, to obtain the appropriate recommendations on the subject matter. You will need to send consultations to the authors included in the email chains. Once the consultations come back, recommendations will then need to be highlighted.

13.4.7 Recording Recommendations of the OPI

Due to their familiarity with the emails, the OPIs must review and provide recommendations on the Phase [illegible] emails that have been gathered. There is no need for OPIs to identify specific provisions of the Act as a basis to redact certain information as ATIP will do so. However, in order for the proper exemption to be applied, the OPI must advise ATIP of any adverse implication and provide rationale for any recommendations provided.

Prior to your review of the records, it is important to highlight in yellow highlighter any recommendations submitted by the OPI in redaction. To do this, select the highlighter icon at the top of your screen in redaction and highlight the area the OPI has recommended to be exempted. If an entire page is to be withheld, a highlighted line down the entire page is sufficient. For consistency within the division, always start with [illegible] highlight for OPI recommendations.

Using the document index to add notes is helpful when your Team Leader is reviewing the file. Adding remarks are especially helpful in the case where more than one recommendation are on the page (i.e. if you have also consulted with another area for recommendations). To record remarks, press the [illegible] icon at the bottom right of the **Redaction** screen. This opens the Document Index area; select the **Notes** tab, and then press the **Document** button. The area will turn white and you will be able to enter the text. Press **Stamp** to place the date and your user ID and then type in your comments. Press **Save** when you are finished with your comments.



13.4.1 Agree / Disagree/ Resolving Recommendations

Since this is a True Access file, you are required to follow the same process, as explained in the Agree / Disagreement / Resolving Recommendations section, under True Access Files, prior to submitting for approval.

13.4.2 Response Letter – Phase 2

RESPONSE

Prior to submitting Phase 2 for approval, you will want to prepare your response letter. The chapter Preparing Your Response Letter provides instructions on how to create your letter. Phase 2 you will use the regular response letter.

13.4.3 Flags

HEADS-UP Formal to LEGAL (Director Approval)

HEADS-UP Formal to (+)

HEADS-UP Informal to:

Since this is a True Access file, you are required to follow the same process, as explained in the chapter on Flags prior to submitting for approval.

13.4.4 Uploading onto the Public Safety Portal (True Access Only)

Once, all approvals have been done and the file is ready for mail out, you must upload your release package onto the Public Safety Portal. The chapter Uploading onto the Public Safety Portal gives more in depth instructions on these steps.

13.5 Access Consultations (ACs) or Privacy Consultations (PCs)

When an Other Government Department (OGD) receives an ATIP request in which the documents contain information that either originated from or pertains to the CBSA, the OGD will send these document(s) to CBSA to seek our recommendations.

When these documents are received by our office, a new ATIP file is opened (Access Consultation (AC) for documents being requested by the OGD through the *Access to Information Act*, and Privacy Consultation (PC) for documents requested under the *Privacy Act* (PA)). The Analyst will then determine which OPIs will need to be consulted and send out a tasking.

The records will then be forwarded to the LO(s) either by placing it in an Apollo folder or by a mailed CD/hardcopy. The records are rarely forwarded via email due to the security classification and the size of the file. The LO(s) will forward it to which Office of Primary Interest(s) (OPI) they feel would need to offer feedback on the documents. The OPI(s) will then send their recommendations to the LO(s) who will in turn, send it to the ATIP Analyst. The file will be reviewed and processed in the same manner as an Access to Information or Privacy Request or Time Access request. The only exception is how we respond (see below) and the recommendations that will be sent to the OGD as our response.

13.6.1 Due Date

If no due date is indicated by the OGD, determine one based on number of pages, type of file and the OPI. If the OGD requests a response by a specific date, determine if it is reasonable based on number of pages, type of file and the OPI. If the due date is unreasonable once you look at all factors at play, contact the OPI and negotiate a new due date with them. More often than not they are happy to comply.

UPDATED CONSULTATION TIMELINES FOR CANADA BORDER SERVICES AGENCY

- 1 to 45 pages – 30 days
- 46 to 100 pages – 60 days
- 101 to 200 pages – 90 days
- Over 200 pages – discuss with your TL or Assistant Director

13.6.2 RESPONSE LETTER

RESPONSE Consult

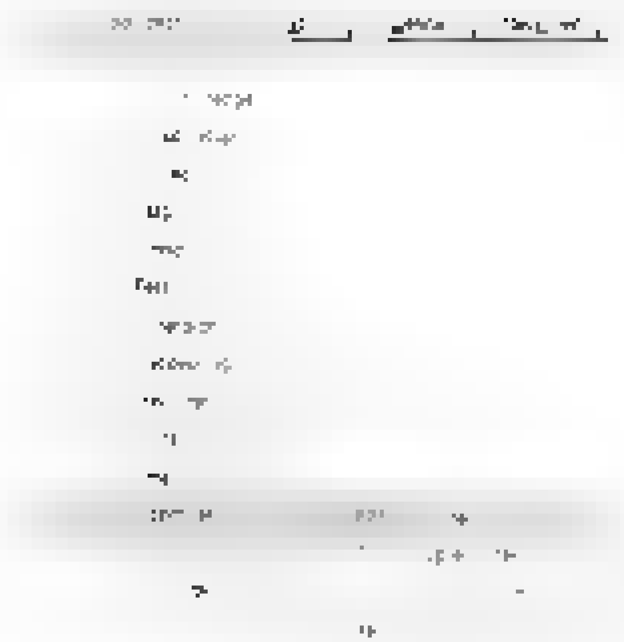
The response procedure for ACs and PCs is slightly different than a client request.

For files where we **have No Objections** to a release, or that we request are **Fully Withheld** we provide our response to the OGD with a signed letter via email. If we have recommendations, we provide our response to the OGD with a letter and recommendation package, both sent via Speedy. All responses sent to OGDs are sent via Speedy.

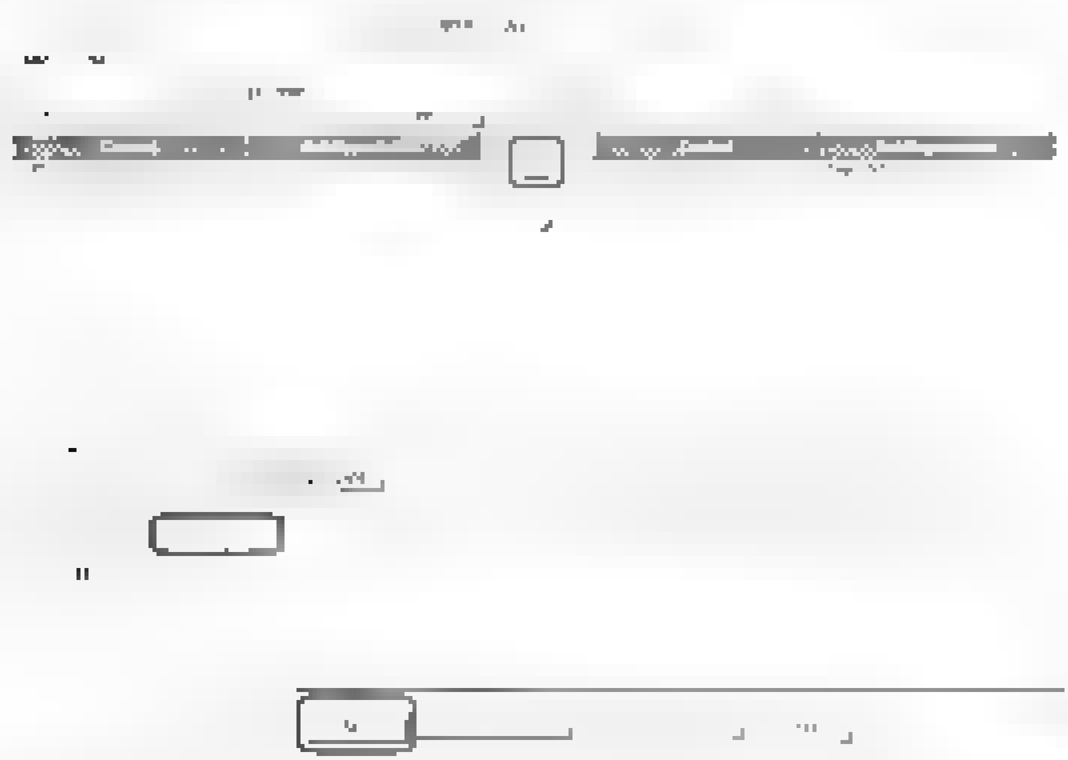
To create the response letter, go to Add Action, select R – **Response** and then **RESPONSE Consult.**

Once the Add Action box pops-up, you can enter the Date Completed as today's date, and place a comment indicating you sent via Email or via Speedy if that is applicable. Once complete, press **Save and Letter**.

Once the letter has been created, you can add an approval action for your Team Leader in order to submit it to them for approval. To add an approval action go to Add Action, select **Approval** and then **APPROVALEmail**



In the Action screen, Add your TL by using the Name Search, and pressing > to bring their name to the right hand side. Leave the Date Completed empty and press **Save**.



Once the Response Consult and Approval actions are in APCM, the file is ready for approval.

When there are **No Objections** or when we recommend that records be **Fully Withheld** in our final response, the delegated officer (your TL) will click on the Response Action and use the email button to send a response via email to the OGD.

<u>Note</u>: The delegated officer will need to put the file back in the Analyst's name prior to generating the email or at least before closing it (for reporting purposes). They will also verify the closing screen to ensure that the information is accurate and input the closing date to conclude the file.

For a **Partial Release** (one in which you have recommendations), a template letter can be found under the Response Consult action by pressing the **Letter** button. Procedures are the same as for regular response letters.

13.5.3 SECRET Records

When there are SECRET records, the Team Leader will return them to the Analyst, who will file them in the in the respective drawer of the secret cabinet 57. It is important to leave a comment in the Document Type action stating where you placed the secret documents. Once the comment has been inputted, close the action.

13.6 Internal Vettings

Occasionally requests are received internally, in which an internal document requires review prior to release to an individual(s). Examples of these are harassment complaints (PV – Privacy Vettings), or website content (AV – Access vetting).

We only provide vetting services for the respondent(s) and complainant(s) involved in personnel investigative proceedings and limit the vetting services solely to the final reports, excluding any evidentiary appendices or emails.

<u>Note</u>: Should a respondent and/or complainant wish to obtain a copy of the complete file, they should be directed to file a formal request with the ATIP Division. Similarly, should any person other than the respondent or complainants want a copy of the report or the file, they should be directed to file a formal request with the ATIP Division.

When one of these requests are received, a new ATIP file is opened (PV or AV), and processed the same way as an external request. For vettings related to Access documents, records which may be disclosed on a public forum, it is likely that the Analyst will need to determine which

LO(s) need to be consulted. Privacy vettings such as harassment complaints are less likely to require internal consultations.

For any consults, the records will be forwarded to the LO(s) either by placing it in an ATIP folder in Apollo, or by mail in CD/hardcopy format. The records are rarely forwarded via email due to the security classification and the size of the file. The LO(s) will forward it to which Office of Primary Interest(s) (OPI) they feel would need to offer feedback on the documents. The OPIs will send their recommendations to the LO(s) who will, in turn, send it to the ATIP Analyst that sent out the original tasking.

13.8.1 Acknowledgement of Receipt and Due Date

ACKaccept

Upon receipt of a vetting request, you first need to determine how many pages need to be vetted. To do this, analyze the request text, as Privacy Vettings often contain multiple recipients, meaning you will need to vet the records separately for each individual (ie. a 10 page request for 4 recipients would amount to 40 pages of records to vet).

Next, based on the below ATIP Vetting Service Standards enter (or verify) the due date in the Edit screen of APCM. To edit the due date, click on the Edit button in APCM and manually change the Due Date there, if required. If you do not have access to edit the Due Date, see your Team Leader.

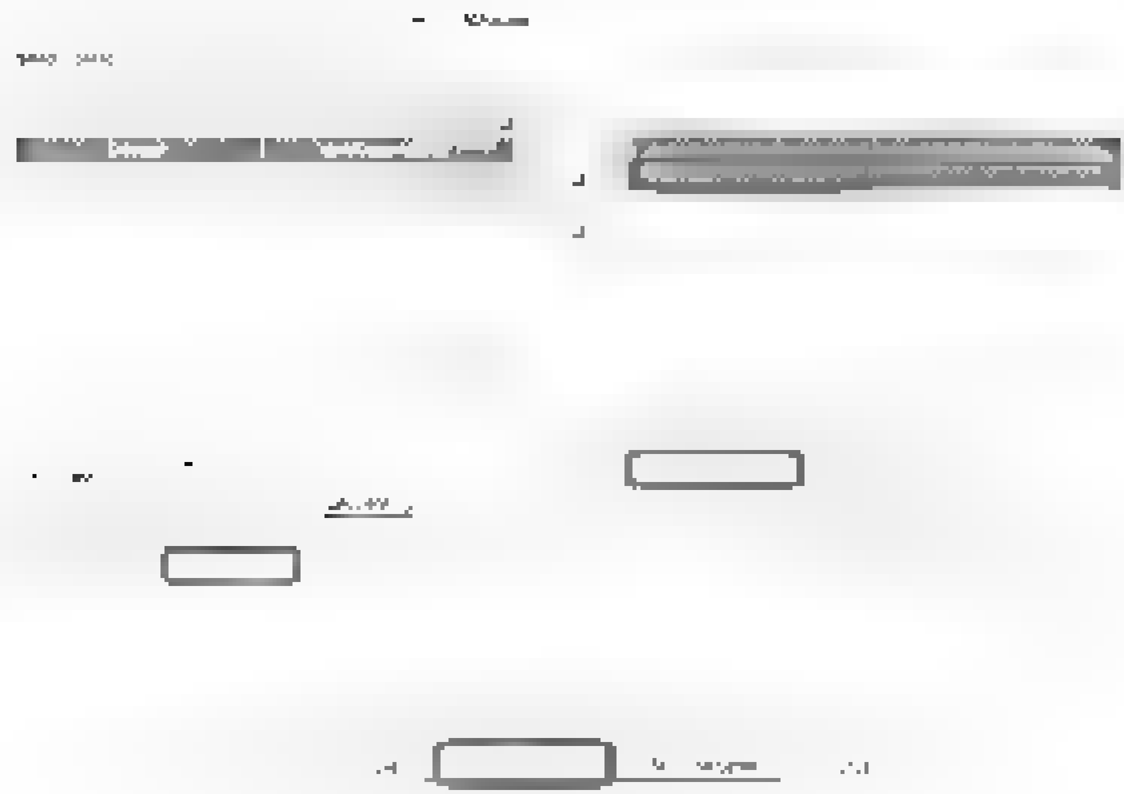
Our vetting service standards are:

- From one (1) to 50 pages – 15 working days
- From 51 to 100 pages – 40 working days
- Over 100 pages, please contact the ATIP and Privacy Division for a time estimate

Next, you will need to send an Acknowledgment email to the requester.

To do this, go to Add Action, ACK – Acknowledge and then ACKaccept.

Once the Add Action box has popped up, enter the Date Completed as today's date. Enter a comment such as "ACK sent" with the date and your initials, then click on **Requester** and then **Save and Email**.



An email template will pop-up. Replace the body of the email with the below message. Do not forget to add your signature to the bottom of the email and change the subject of the message.

SUBJECT: Acknowledgement of your Vetting Request -AV-2018-XXXXX

English Version – la version française suit

The ATI and Privacy Division provides the service of informally severing CBSA records, for internal programs, as if they had been requested under the *Access to Information Act* or the *Privacy Act*. In particular, this service is routinely offered as part of the vetting of Professional Standards Investigations Reports and Harassment Reports.

Should you require the ATI and Privacy Division to review records in accordance with the requirements of the *Access to Information Act* or the *Privacy Act*, the turnaround times are as follows:

From one (1) to 50 pages – 15 working days
From 51 to 100 pages – 40 working days
Over 100 pages, please contact the ATI and Privacy Division for a time estimate.

Note: Additional time may be required due to the complexity of a file or the requirement to undertake external consultations. If your request is urgent, please contact the ATI and Privacy Division to make alternate arrangements.

To better manage such requests, the ATIP Division will only provide vetting services for the respondent(s) and complainant(s) involved in personnel investigative proceedings and will limit the vetting services solely to the final reports, excluding any evidentiary appendices or emails. Should the respondent(s) and/or complainant(s) wish to obtain a copy of the complete file, they should be directed to file a formal request with the ATIP Division. Similarly, should any person other than the respondent(s) or complainant(s) want a copy of the report or the file, they should be directed to file a formal request with the ATIP Division.

These changes will allow us to provide you with the final vetted reports as expeditiously as possible, which in turn will assist you to resolve the situation with the parties that are directly affected and enable the ATIP Division to provide a greater level of service to other clients.

Should you have any questions please contact Dan Proulx, Executive Director, ATI and Privacy Division at 343-291-6069.

Thank you.

* * * * * * * *

Version française – English Version Precedes**

La Division de l'accès à l'information et de la protection des renseignements personnels (Division de l'AIPRP) offre des services informels de caviardage des documents de l'ASFC pour les programmes internes, comme s'il s'agissait d'une demande soumise au titre de la *Loi sur l'accès à l'information* ou la *Loi sur la protection des renseignements personnels*. Ce service est notamment utilisé de façon régulière pour les rapports d'enquête relatifs aux normes professionnelles et les rapports relatifs au harcèlement.

Si vous voulez que la Division de l'AIPRP examine pour vous des documents en conformité avec les dispositions de la *Loi sur l'accès à l'information* ou la *Loi sur la protection des renseignements personnels*, veuillez noter que les délais de traitement sont les suivants :

Documents de 1 à 50 pages : 25 jours ouvrables
Documents de 51 à 100 pages : 40 jours ouvrables
Documents de plus de 100 pages : veuillez communiquer avec la Division de l'AIPRP pour connaître le délai approximatif de traitement

À noter que suivant la complexité des documents ou la nécessité de consulter des entités externes, les délais susmentionnés pourraient être prolongés. Si votre demande est

présente, veuillez communiquer avec la Division de l'AIPRP pour prendre les dispositions nécessaires.

Afin de mieux gérer de telles demandes, la Division de l'AIPRP n'offrira ses services de caviardage qu'aux intimés et aux plaignants concernés par une procédure d'enquête sur le personnel et seulement pour les rapports définitifs, ce qui exclut les courriels et les documents de preuve en annexe. Si les intimés ou les plaignants souhaitent avoir une copie complète du dossier, ils devront présenter une demande en bonne et due forme à la Division de l'AIPRP. De la même façon, toute autre personne désirant une copie du rapport ou du dossier devra aussi soumettre une demande officielle à la Division de l'AIPRP.

Ces changements permettront à la Division de l'AIPRP de vous fournir la version caviardée des rapports définitifs dans les plus brefs délais, ce qui vous aidera à régler les différends avec les parties directement concernées et permettra à l'équipe de la Division d'offrir ses services à un plus grand nombre de clients.

Pour toute question, veuillez communiquer avec Dan Proulx, directeur exécutif, Division de l'AIPRP, au 343-291-6969.

Nous vous remercions de votre collaboration.

13.6.2 Review

REVIEW

The review of a vetting file is the same as the review of any type of file, the steps being check notes, highlight recommendations, and then redact. But in an Access Vetting, like a True Access request, cannot be closed until an agreement is reached on all recommendations provided by the OPIs. As an Analyst, you may propose to sever more information. If the OPI has asked that something be exempt and you disagree, you need to work with the OPI and come to an agreement on what will be redacted.

The chapter Reviewing Records, provides further explanation on the Review Stage.

Communicated with

The **Communicated with** action, can be used to record any back and forth between yourself and the requester. This action is located under **Add Action**, then in – **Processing**.

13.6.3 Response Letter – Privacy or Access Vetting

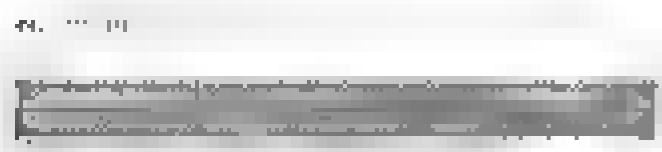
RESPONSEPrivacyVetting

Before your response letter is prepared you will need to do your closing screen. Instructions on those steps can be found in chapter Releasing Records, specifically section [illegible].

To prepare a response letter for a vetting, go to Add Action, select E - Response and then **RESPONSEPrivacyVetting**.

Vettings can be responded to by courier (Speedy), hand delivered or when possible by email. Once your Add Action box has opened, indicate the manner in which you responded in the comment box, enter the Date Completed as today's date, click on **Requester**, and then **Save and Close**.

Select the chat Template you require and then press Select.



Your response letter will now appear. Please verify that it is the correct recipient and that the address components are in the correct order:

- Full name
- Street address, Apt #
- City, Province 'QC', postal code
- [REMOVE 'CANADA' at the end of address]

Ensure that Mr. or Ms. is before the last name. However, if you are unsure of their gender write their full name instead.

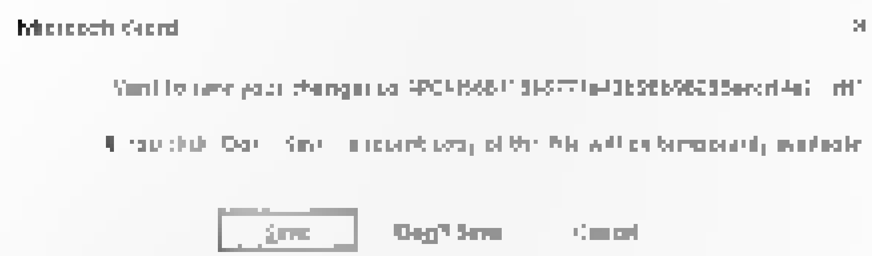
- Ie. Dear Mr. / Ms. Smith
- Ie. Dear Ashley Smith

Verify that the correct Team Leader's name (that will approve) appears above the ATIP address at the bottom of the letter.

Complete the first sentence of the letter to correspond to your vetting request.

For Enclosure, edit to correspond to your vetting request.

Once you are done with your letter, close it and you will be prompted to save, press **Save**.



Complete the letter Attachment box with "letter" in the Description and press **Attach**.

Next, you will submit your file to your TL for approval. For additional information on these steps, reference the chapter Approval of File.

If sent by email – Once approved, the delegated official (your TL) will click on the Response Action and use the email button to send a response via encrypted email (including records attached) to the internal contact for the request.

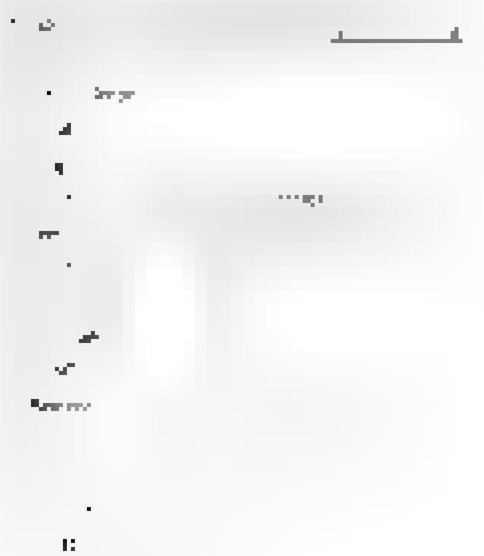
<u>Note</u>: The delegated officer will need to put the file back in the Analyst's name prior to generating the email or at least before closing it (for reporting purposes). They will also verify

the closing screen to ensure that the information is accurate and input the closing date to conclude the file.

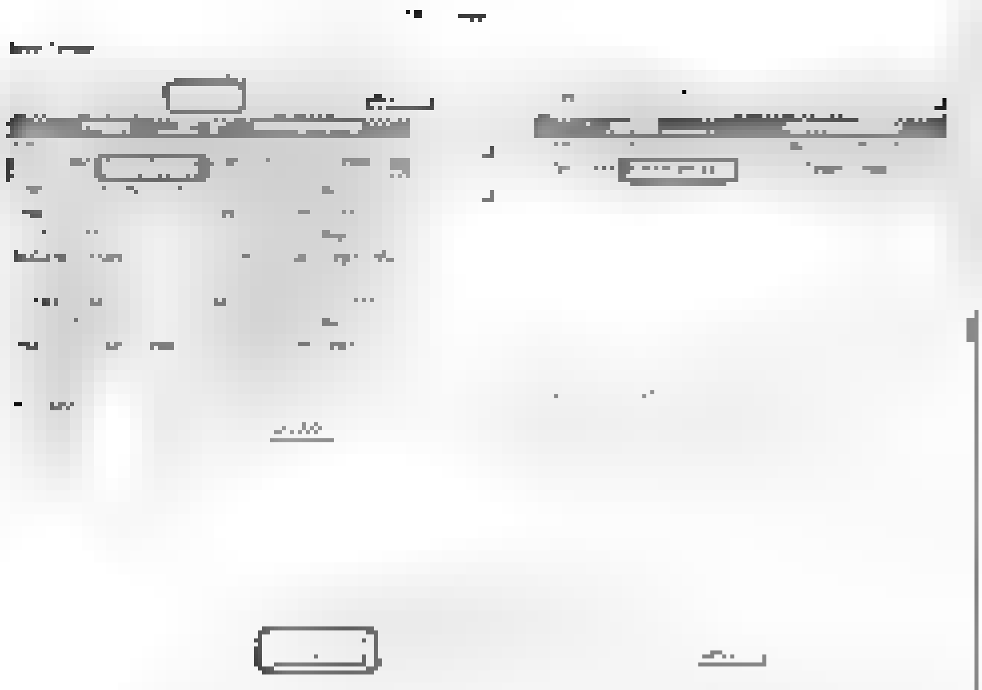
If the response is being hand delivered or sent via courier, the file will be returned to you after it has been signed off by a Team Leader. You will then prepare the release package and send for mail-out as you would any regular release package.

14. SENDING RETRIEVALS

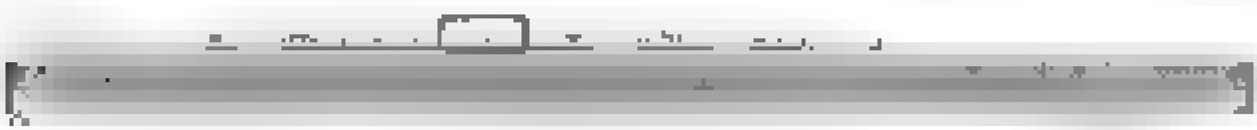
To send a RETRIEVAL, click Add Action, then E - Retrieval and select **RETRIEVAL notice**



Once the Retrieval Notice action opens, type in the area that you wish to task in the Unit/Organization block, and press > to bring it to the right hand side. Add as many areas as you wish to task and bring them all to the right hand side of the action box. You may type in "retrieval sent" with today's date and your initials. Leave the date Completed blank until the you receive a response from the LO, and press Save.



Next, you will want to select a RETRIEVAL notice and press Email



Select your email template. Chose **Retrieval Email** and press **Select.**

Your email will now pop up, and all areas that you have previously selected in your retrieval actions will populate into your email "to" field.

If you are tasking a region for a client's records, GCMS and ICES clippings should be included in your email to indicate where the information might be held. To do this see ANNEX E: TIPS AND TRICKS. If you are tasking multiple areas, the clippings should ONLY be sent to the region concerned. Do not send it to other areas (delete the other areas in your email in the "To" field). You may be sending multiple retrieval emails, depending on the request and regions needed to be tasked.

Next, remove the [illegible] privacy brackets, and review the text for any errors. Add any special instructions (if needed) at the top of the email. Make sure that you press **encrypt** at the top of the email, and then press **Send.**

5)

Note: It is important to **Print to Redaction** all of your emails (including retrievals) into the ADMIN stack. You should go into your In-box – sent items to print your retrieval email into Redaction.

Organize your admin file (and later any records) by stacking and indexing them. Printing to Redaction, Stacking and Indexing explains how print to Redaction, set up your printer and

organize your items in Redaction. Annex ... Tracking and Indexing shows the various naming conventions used in our group.

14.1 Clarification after Tasking

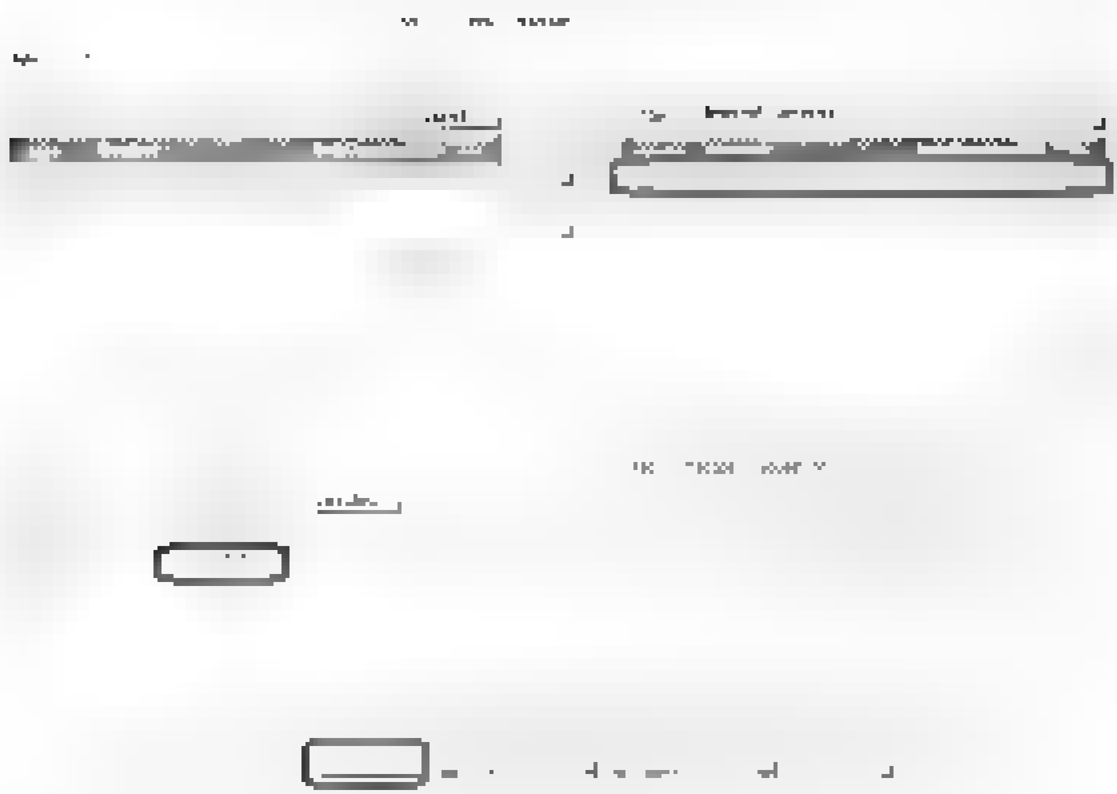
Sometimes, the OPI may seek out clarification on our tasking. When communicating on matters within the file it is good practice to use the Action **Communicated with:** to record notes of these communications.

Communicated with

To add the Action, go to **Add Action**, then **II- Processing** and select **Communicated with:**

You can use this action to record any communications. For communications with your applicant you can select **Requester** on the left hand side of your Action box and press > to bring it to the right. Enter the **Date Completed** as today's date, and place any relevant notes in the **Comments** field. Press **Save** when complete.

Note: Every time you add new communications to this action field, you should update your **Date Completed** to the current day.



For clarifications regarding the tasking: if an OPI has already been tasked and further clarification is now required from the applicant, the Analyst should:

- Ask the OPI how the retrieval of the records could be facilitated. For example, are there any records that can be pulled easily (i.e. reports, working papers).
- Let the OPI know that you will clarify the request and ask them what types of options should be proposed to the applicant (i.e. narrow scope, timeframe, request key documents instead of all documents, etc.).
- If it becomes too difficult to clarify the request, and you find that you have to go back and forth between the applicant and the OPI, you can put the requester and the division directly in contact (if the applicant and departmental officials agree). You should first discuss this method of communication with your Team Leader/Assistant Director before you proceed.

In cases where you realize that you must obtain further clarification from the applicant on the scope of the request before you can proceed:

- Advise all OPI's that a request for clarification is being sought from the applicant and to stop all work regarding this request and to consider the tasking closed;

- While you are trying to clarify with the applicant, the taskings to the OPI should be closed.
- If you try to reach the applicant by phone and you have to leave phone messages, let them know that you are calling for a clarification on his/her request and that the request is on hold until you can get that clarification. Ensure that you record all attempts of contacting the applicant on your file in APCM.
- If clarification took place verbally, send a follow-up email or ACKaccept letter (modified accordingly) to the applicant to document the revised wording.
- If the applicant is not easily reachable by telephone send an ACKincomplete letter, modify it if needed.
- Once you have clarification, send a new tasking email (with new deadline) to the appropriate OPI(s) with the clarified wording of the request.
- If the applicant fails to respond to our formal request for clarification before 30 days (45 as a courtesy), the file will be considered abandoned by the applicant and you will proceed to close the file.

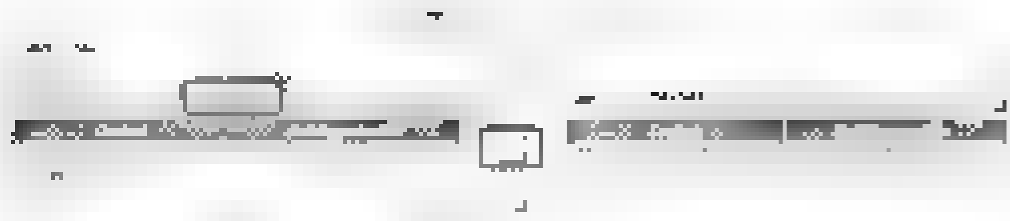
14.2 No Response to your Retrieval?

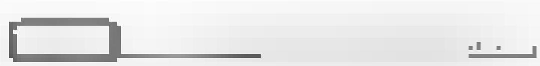
If a/the OPI has not responded to the tasking by the date the tasking was due, follow up.

Follow-up

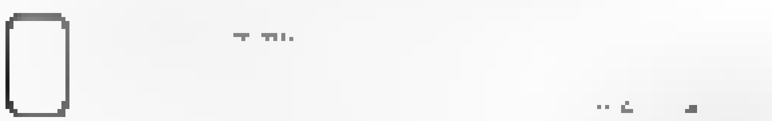
Select Add Action, 1 = **Other** and then **Follow-up**

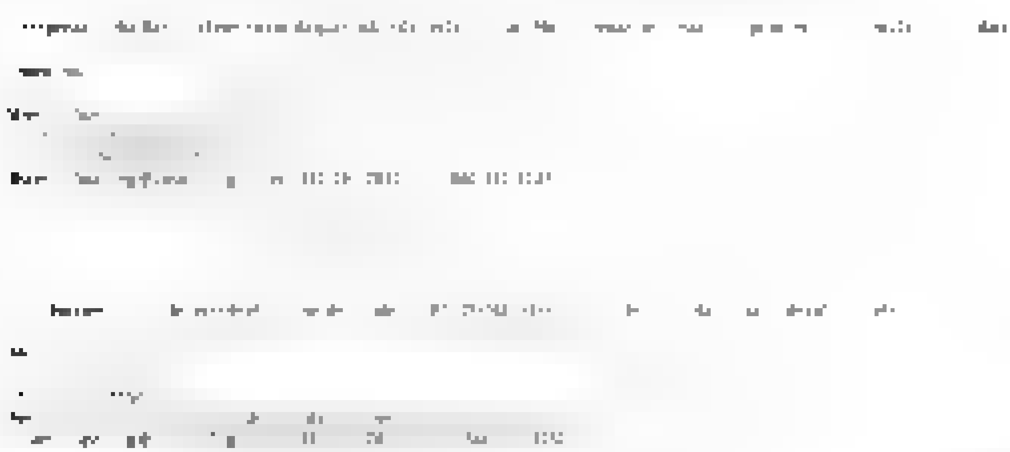
Input the region/branch that you are following up with in the Unit/Organization and press **Search.** Once it populates below, press > to bring it to the right hand side. The date completed is today's date, and input a comment such as "followed up by email", the date and your initial in the comment field. Once complete, press **Save.**





Once back on your main screen, select the Follow-up action line and press Email. A template email will populate, you can go ahead and Send.

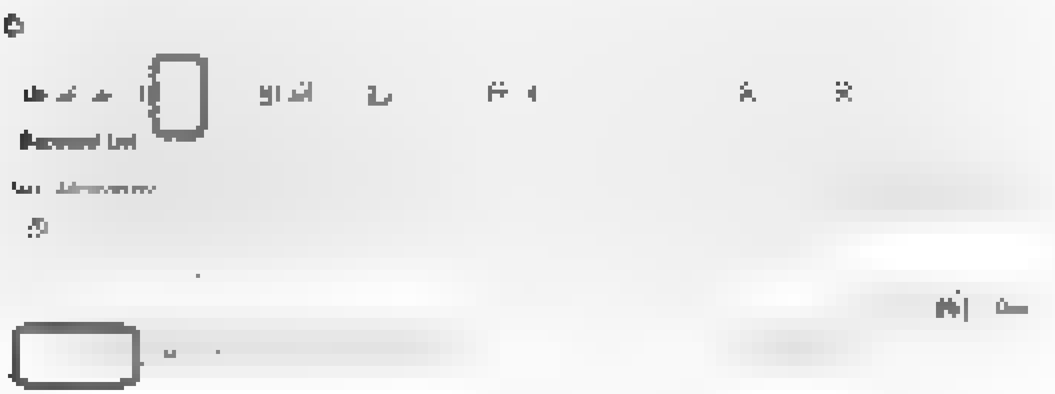




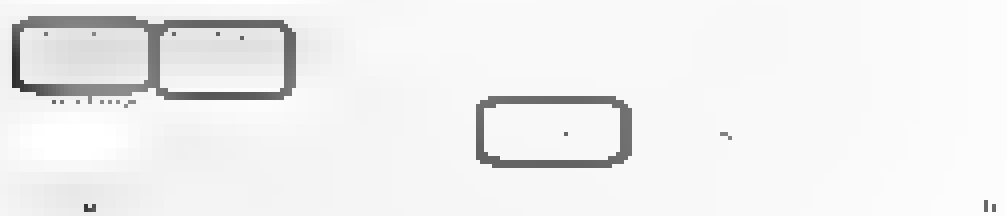
If after a few days they still don't reply, go ahead and escalate the issue to your Team Leader

15. PRINTING TO REDACTION, STACKS AND INDEXING

In Redaction, click on the Stacks button and click New.



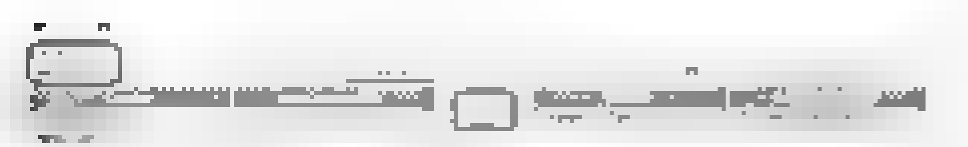
Add your stacks using the naming conventions as shown in Appendix C.

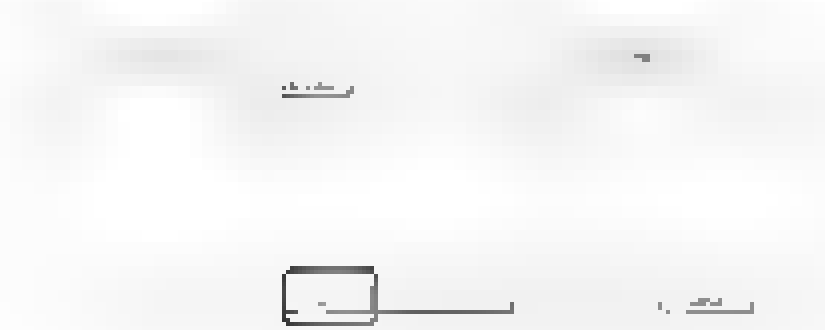


Paper is always scanned into redaction by our administration team. If you receive paper records/documents that haven't made it into Redaction, you can create an action for the administration team to scan the documents (create your own stacks before you send it off for scanning).

To create this action, select Add Action → Processing and then Scan/Index

Type in "Operations" in the Name field and press Search. Select **Operations Team** and press > in order to bring it over to the right hand side as shown below. Also record in the Comments field the date requested and your initials. The Date Completed remains blank until the action is completed by the Operations team. Then press Save.





Most records come in electronically on Apollo

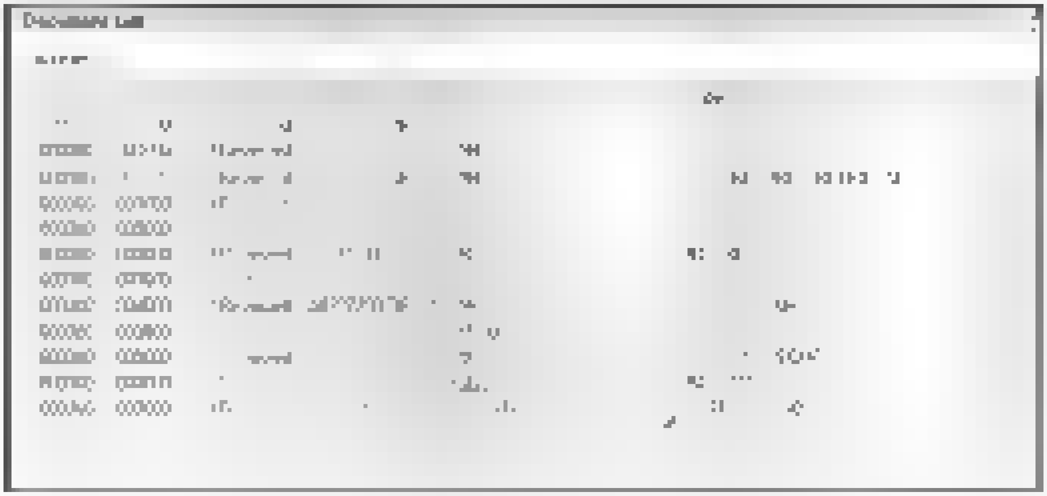
You can print these records into Redaction yourself. To do this, open the file and select **Print** and then "Print to Image" as your Printer (also see Changing Printer Properties). You can select multiple stacks by holding down the Ctrl key, then press **OK**.

Once your records are in Redaction, you can index each tiff. To do this, click on the button at the bottom right of your Redaction screen.

Once your Document Index opens, press **Document**. You can now type in a small description of the tiff in the Subject field. Once you are done, press **Save**. This is a great way to mark important components of your file, to assist your Team Leader when they are reviewing the file.

Add your Subjects using our naming conventions as shown in Appendix D: Naming and Indexing.

An example of a file is shown below; you can see how certain tiffs will be linked to several stacks.



Note: Never under any circumstances, print SECRET or TOP SECRET documents (anything above Protected B) into Redaction. Records that are SECRET or TOP SECRET will remain as hardcopy components of the file until they are treated. Only once the appropriate redactions are made (on our standalone computer or taped) and approved, can the redacted version be scanned into Redaction. See Annex H: Information Classification Guide.

During the processing of the file, SECRET or TOP SECRET documents should be stored in the appropriate temporary docket and locked in the approved-style cabinet (located in our SECRET room) whenever not in use.

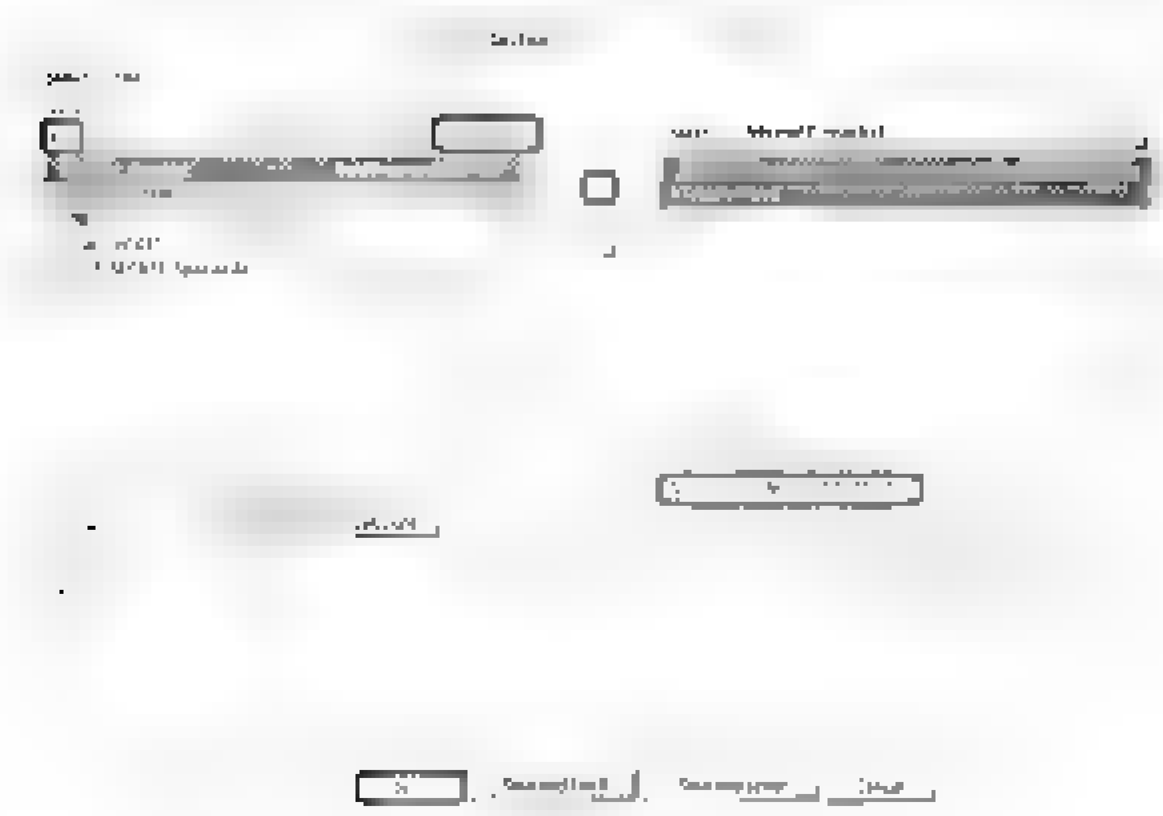
Files with SECRET or TOP SECRET records should be flagged appropriately in APCM using the **DocType (h): Action**. This is important as it notifies Analysts and Team Leaders that there are additional records aside from those already in redaction. For more information on how to manage these types of records please see Managing SECRET Records.

You can also use the **DocType (h): Action** to indicate when multimedia records exist on your file such as audio and video.

To do this, Add Action "H – Processing" and select DocType (h).

DocType (h)

By typing "h" into the Name field, and pressing **Search**, you are able to select the relevant document type that is on your file. Highlight the type and press > to bring it over to the right. It is important to indicate the number of pages, type of records, and location of records in the Comments field. Leave the Date Completed blank and press **Save**. This action will be closed later on when the file is closed.



16. REVIEWING RECORDS

If you haven't already input your records into Redaction, stack and organize them. The section Printing to Redaction, Stacking and Indexing explains how print to Redaction, set up your printer and organize your items in Redaction. Annex C, Stacking and Indexing shows the various naming conventions used in our group.

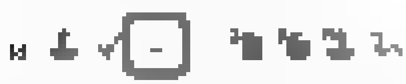
Your next step is to record any recommendations that came in with the retrieval.

16.1 Recording Recommendations of the OPI

Due to their expertise in the information, OPIs review and provide recommendations on the records they have submitted. There is no need for OPIs to identify specific provisions of the Acts as a basis to redact certain information as ATIP will do so. However, in order for the proper exception to be applied, the OPI must advise ATIP of any adverse implications and provide rationale for any recommendations provided.

16.1.1 Highlighting in Redaction

Prior to reviewing the records, it is important to highlight (in yellow highlighter) any recommendations submitted by the OPI into redaction. To do this, select the highlighter icon at the top of your screen in redaction and highlight the areas that are recommended to be exempted. If an entire page is to be withheld, a highlighted line down the entire page is sufficient. For consistency within the division, always start with YELLOW a highlight for OPI recommendations.

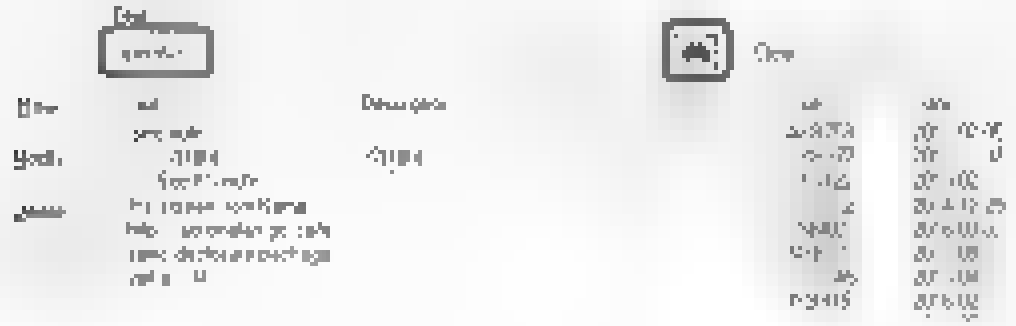


If you have several recommendations from different OPIs, you may colour code your highlights. It is important to note which highlight belongs to what OPI, either with a custom stamp, or the document index.

16.1.2 Custom Stamps

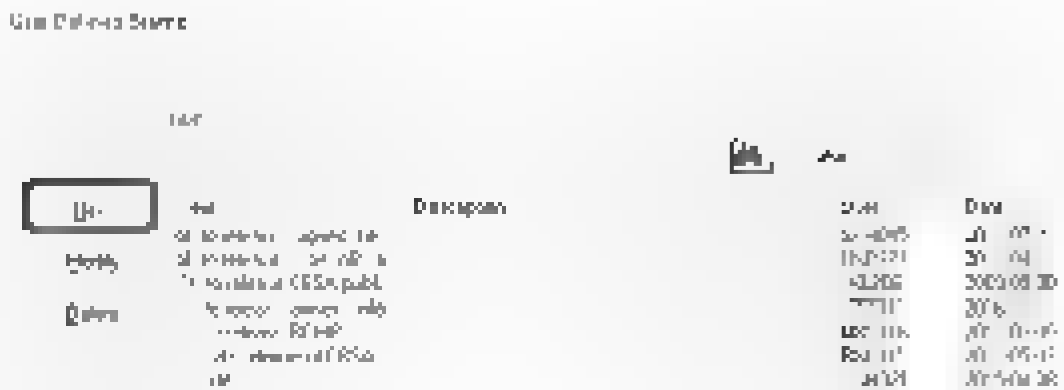
To create a custom stamp, select the **User Defined Stamp** in Redaction.

First, search for a previously created stamp. To do this, type in the text that you are seeking (or a portion of the text) and press the binoculars to perform the search.



If you find what you are looking for, click on it and press Stamp.

If the stamp isn't there, create your own by clicking on **New**.

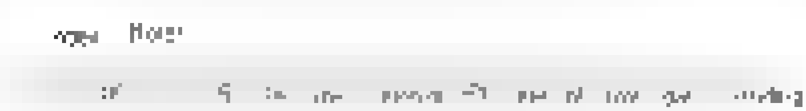


Type the name of the New Stamp in the Text box and press **Save Close** when complete.

Select User Defined Stamp again in Redaction and search for your newly created stamp. Once found, select and press **Stamp** to use it. You may use these custom stamps to stamp any text that you feel will help a reviewer navigate through your file.

10.2 Recording Notes in Redaction

Using the document index to add notes is helpful when your Team Leader is reviewing the file. Adding remarks are especially helpful in the case where more than one recommendation are on the page (i.e. if you have also consulted with another area for recommendations). To record remarks, press the icon at the bottom right of the Redaction screen. This opens the Document Index area. Select the **Notes** tab, and the press the **Document** button. The area will turn white and you will be able to edit the text. Press **Stamp** to place the date and your user ID and then type in your comments. Press **Save** when you are finished with your comments.



16.3 Triaging Records

Scan records for:

- Obvious duplicates and/or Not Relevant records
- Missing attachments – Flag any documents that appear to be missing attachments for further investigation. The attachments will need to be retrieved from the responsible OPI
- Possible consultations – Note if records concern or originate from other government departments or other levels of government, and note if records contain possible cabinet confidences
- Possible third party consultations – Note if records originate from a third party.

If records that need to be consulted on have been found, or if the records are voluminous, an extension should be taken on the file.

If your file has SECRET records, they should not be scanned into Redaction. Please see Managing Secret Records for more information on how to process SECRET records.

16.4 Extensions

Both the Privacy and Access to Information Act allow for a legal response time of 30 calendar days from the date of receipt of an official request. However, this period may be extended for limited and specific reasons identified in the Act. Common reasons for an extension to be taken include volume, complexity and the need for consultation, and these can be identified during the initial review process of the file. Please see the chapter Applying Extensions and Sending Consultations for more information.

16.5 Exemptions and Exclusions

The Access to Information Act (ATIA) and the Privacy Act (PA) provide the public with a right of access to information held by federal government institutions. These rights of access are subject to very limited and specific exemption. Unless the information can be legitimately withheld under a specific provision of the Act, the information must be disclosed.

See Privacy Act Articles and Access to Information Act Articles for a list of exemptions and exclusions under each Act.

16.5.1 Exemptions

Sections 13 through to 24 of the ATIA and sections 18 through 28 of the PA set out a number of exemptions to the right of access under these Acts. Sections 68 and 69 of the ATIA and sections 69 and 70 of the PA describe the types of information to which the Acts do not

apply. These form the only basis for refusing access to government information requested under either Act.

<u>Mandatory vs. Discretionary Provisions</u>

Exemptions fall into two distinct categories: mandatory and discretionary. Mandatory exemptions are introduced with the wording "... the head of a government institution <u>shall</u> refuse to disclose..." which indicates there is no option but to refuse access to the information.

Discretionary exemptions are introduced with the wording "... the head of a government institution may refuse to disclose ..." In these instances, the institution has the option to disclose or protect the information.

<u>Injury vs. Class Provisions</u>

Mandatory and discretionary exemptions fall into two categories: injury test and class test; they can be either mandatory or discretionary in nature. Class-based exemptions apply where the information falls within the class of information described in the exemption and there is no reference to any consequence that might result from the release of the information. When injury-based exemptions apply, an injury must be demonstrated before the exemption can be claimed.

16.6.2 Exclusions

Exclusions are found in sections 68 and 69 of the ATIA and sections 69 and 70 of the PA. In accordance with these sections, the Acts do not apply to:

- Published material or material available for purchase by the public, library or museum
- Material or material made or acquired and preserved solely for public reference or exhibition purposes
- Materials placed in the National Archives of Canada, the National Library, the National Gallery of Canada, the Canadian Museum of Civilization, the Canadian Museum of Nature or the National Museum of Science and Technology by or on behalf of persons or organizations other than government institutions
- Confidences of the Queen's Privy Council for Canada, including:
  - memoranda presenting proposals or recommendations to Council
  - policy options to Council for consideration in making decisions
  - agenda of Council, records reflecting communications or discussions between ministers of the Crown
  - briefing material for ministers concerning matters before, or proposed to be brought before Council, and:
  - draft legislation.

Note: Before formally withholding a Cabinet Confidence, ATIP must formally consult on the record in question.

16.6 Reviewing your Records

Once recommendations are highlighted and pages are flagged, you are ready to review the records and apply severances. If any information falls under a specific provision of the Act, it will be exempt. Otherwise, the information must be disclosed.

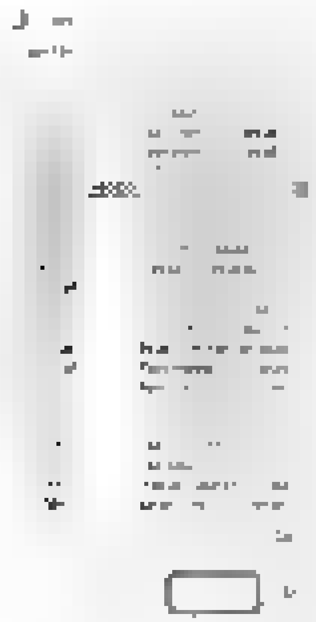
16.6.1 Redacting Information

To sever information from a page, you will want to select the **Scissors** icon at the top of your screen that is with the blue box.

With the scissors selected, highlight the information that you wish to redact. The severing will appear as a pink box on the page.

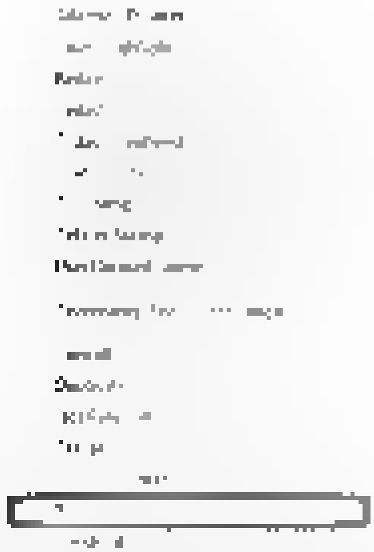
Next click on the **Stamp** button.

This will create a pop-up with a list of the sections of the Act. You will need to select what section of the Act you are removing the material under by clicking on the box on the left hand side of the exemption.



Now will stamp section selected by clicking anywhere on the page. Try not to click area with text that your Team Leader will need to review. Preferably on a blank section of the page. This stamping action will automatically change the disclosure of your page to Partial. This will be displayed on the left hand side of your screen.

If there are no severances required on any particular page, you can right click anywhere on the page and select **Release**.



Once you have reviewed all records provided to you by the OPIs, you will **paginate** these pages.

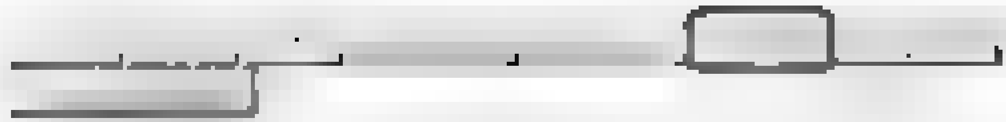
16.5.2 Paginating your Records

Select all of the pages reviewed by either holding down **SHIFT** or **CTRL**. Then right click and select **Pagination** and then **Set Pagination**. This will associate your page with numbers and prepare your file for review. Do not include any ADMIN pages in your pagination.

Next, return to **APCM** to complete the Closing Screen.

16.5.3 Closing Screen

Before your response letter is prepared you will need to do your closing screen. To do this press on the Close button in APCM.



- [illegible] box will pop up. You will fill in the following sections:

Disposition

The final disposition in the [illegible] screen must reflect all releases:

Abandoned by applicant
All disclosed (if nothing was exempted)
Disclosed in part (if you did sever any information)
Does not exist (if there were no records)
Neither confirmed nor denied (if the admission that the information exists/does not exist is information in itself not to be released)
Nothing disclosed – excluded (if all information was excluded)
Nothing disclosed – exempted (if all information was exempted)
Publicly available (if information is publicly available)
Transferred (if the file was transferred to another institution)
Treated informally (Requests are treated informally when it has been determined, through consultation with the applicant that processing a formal request can be discontinued in favour of providing the information informally. A request treated in this manner must be considered to have been abandoned. Ensure your response letter does not include a right to complain paragraph or refer to the Act)

Note: If the first release was all disclosed, but a subsequent release was disclosed in part or nothing disclosed, then the final release package would be disclosed in part.

Method of Access*

Copies given – electronic (if the release is on CD)
Copies given – Paper (if the release is on paper)
Copies with examination (viewing) – paper and release
Examination (viewing) only
Not Applicable (if abandoned, transferred or does not exist).

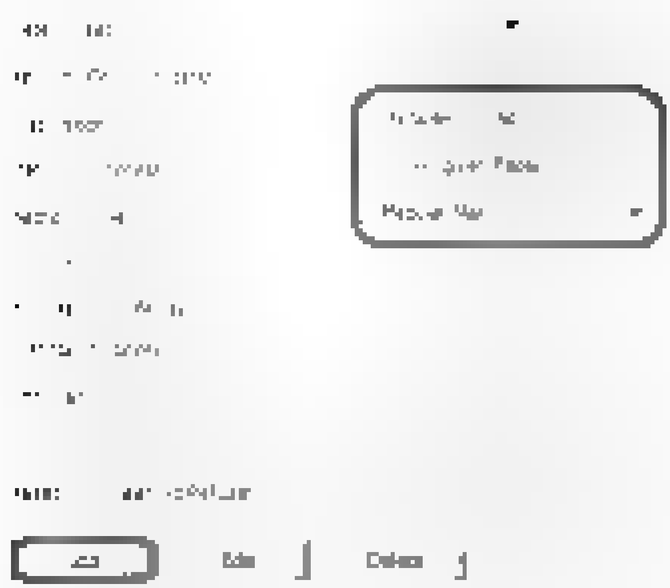
* If the applicant has asked for specific format, you must adhere to their request. If a record is over 50 pages it is provided on CD.

Method of Delivery

Courier (if sent by courier)
Email (if sent by email*)
Faxed (if sent by fax)
Hand Delivered (if hand delivered)
Not Applicable (no records, abandoned or viewing only)

* Personal info should always be encrypted if sent by email.

Once finished press **Add**



Fill in the sections as shown below with the same information as above. You can find the numbers for pages processed off the window below, by dragging the Add Release box over.

Add any manual pages if applicable, under PROCESSED. If a severed copy of the manual pages were added to Redaction (i.e. SECRET pages), there is no need to enter the manual pages as they were accounted for in the electronically processed fields (you will have to count and add withheld pages).

The Release Date should be today's date (the date you are closing the file), and Versions should always be complete.

Press Finish.

You will now see the disposition that you added in the Close Request box.

Press **Finish**, and you are now ready to create your response letter. See the chapter Preparing your Response Letter for more information.

17 APPLYING EXTENSIONS

Both Acts allow for a legal response time of 30 calendar days from the date of receipt of an official request. However, this period may be extended for limited and specific reasons identified in the Acts. For instance, extensions may be taken if:

1. The request is for a large number of records or necessitates a search through a large number of records and meeting the original time limit would unreasonably interfere with the operations of the government institution. A helpful tool in determining the number of days to extend based on volume is below.

Volume Calculation Table	
Number of Pages	Days to extend (all in calendar days)
499 pages	0 days
500 – 999 pages	30 days
1,000 – 1,499 pages	60 days
1,500 – 1,999 pages	90 days
2,000 – 2,499 pages	120 days
2,500 – 2,999 pages	[illegible] days
3,000 – 3,499 pages	180 days
3,500 + pages	See your Team Leader

2. Consultations are necessary to comply with the request that cannot be completed within the original time limit; or

3. Additional time is necessary for translation purposes or for converting personal information into an alternative format.

It is good practice that once you receive the records from your retrieval action, to <u>immediately</u> scan the file for these extension reasons and apply extensions to the file accordingly. You must take an extension within the first 30 days of a completely received request. Do not take extensions if a request has not yet been completely received or on hold for clarification.

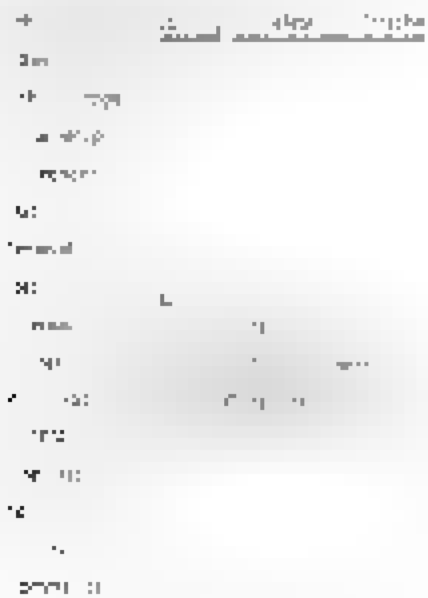
Note: For a *Privacy Act* request, you can only place a 30 day extension.

If any extensions apply, add all relevant extension actions in APCM and indicate the reasons for the extension(s). Make sure to enter the amount of time taken for each extension reason. If more than one extension applies (if you take 120 days total, do not set one to 120 and the other to zero).

Example: For a large volume Access file which also has a consult, you have concluded that you will need 60 days for volume, and 30 additional days for consultation, totaling a 90-day extension.

For Access files, if a time extension is greater than 30 days, we are required to notify the Information Commissioner of the extension.

To add an extension in APCM, go to Add Action, then select @ = Extension and select the type of extension that applies. Add each extension that is applicable.



There are 3 types of extensions available to use in APCM are:

EXTEND Volume

ATIA paragraph 9(1)(a) / Privacy Act 15(a)(i)

Refers to a large number of records and to an unreasonable interference with the operations of the government institution. Both the words "large" and "unreasonable" are subjective terms that may be interpreted according to the circumstance and the context of each specific request.

Generally, more than 500 pages relevant to a request are considered a large number of records. Note: For determining volume if the records are paper based (unscanned), 1 inch of paper equals approximately 200 pages. A request under 500 pages may also be considered a large request if they are deemed complex in nature.

Generally, interference with an institution's operations may be considered unreasonable if processing the request within 30 days would require the following:

- monopolizing a significant portion of the resources of the office of primary interest to the detriment of its core functions; or
- using such a high proportion of the resources of the ATIP Office that it would have a significant negative impact on the processing of other requests.

EXTEND Consultation

ATIA paragraph 9(1)(b) Privacy Act 15(a)(ii)

A "consultation" refers to consultations undertaken within a government institution, with other government institutions or other divisions within the same institution.

An extension may also be justified when an institution must seek legal advice in order to resolve issues related to the processing of a request.

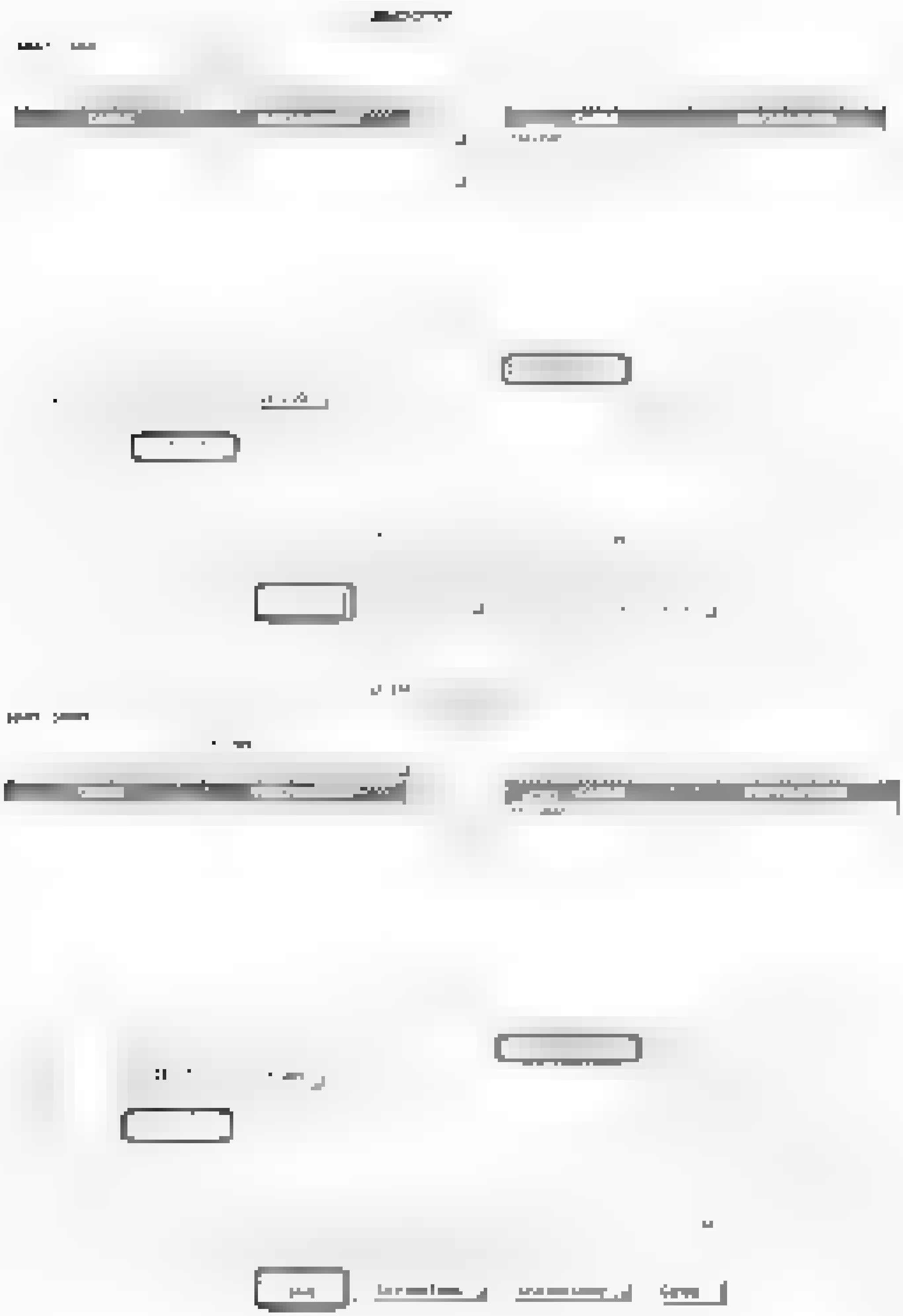
EXTEND 3rd Party

ATIA paragraph 9(1)(c) Privacy Act 15(a)(ii)

Subsection 27(1) of the ATIA requires institutions to send third party notices within 30 days after the request is received. Additionally, 27(4) allows institutions to send subsection 27(1) notices after the initial 30 days when the deadline has been extended under paragraphs 9(1)(a) or (b), that is, within the extended time limit. However, subsection 27(4) does not allow for an extension of the deadline for the processing of the request.

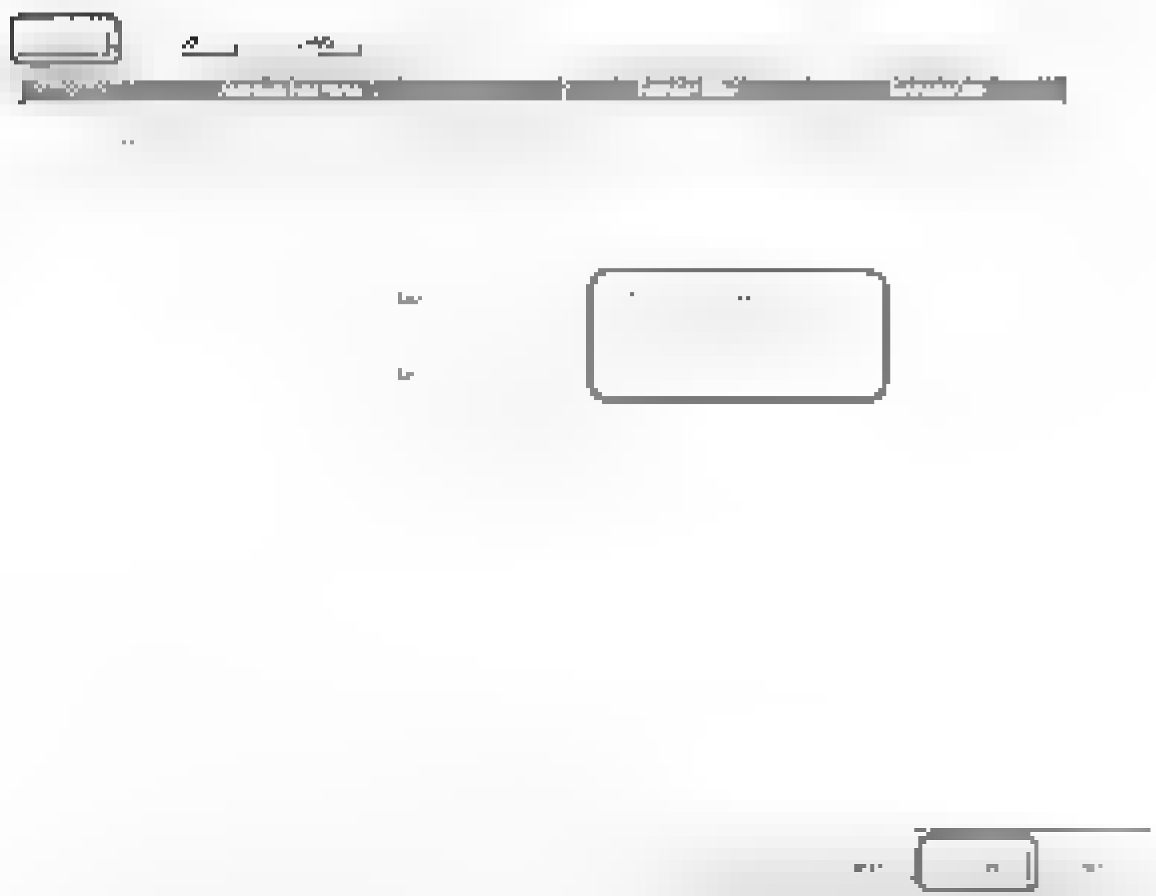
17.1 Adding the Extension in APCM

When adding your extension actions in APCM, record the reason and number of days in the Comment field. You also can close the date completed (put today's date). Then press **Save**.

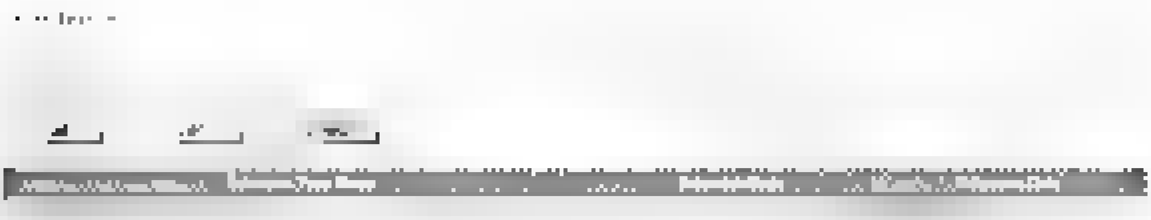


Before you can produce a letter, you will need to also add the days in another area of ARCM

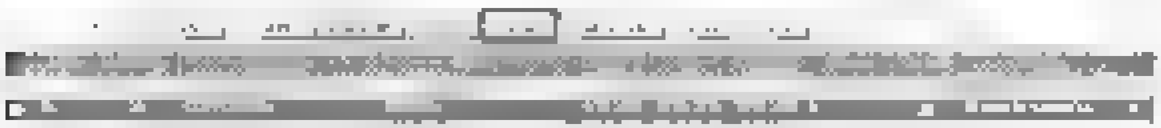
To do this, press the **Extensions** button at the APCM screen. Once you do this a Request Extension box will pop-up. Press **Add** and choose the application extension type to your file. For this example, as you have extended for both volume and consult, you will do this step two times. Add the number of extension days for each type, and today's date as the Extension Date and press **Finish** each for each extension.



After you are done, you should be able to see your extensions in the Request Extension box. Press OK to close. This step populates the number of extension days onto your letter, so you must complete this step prior to creating your letter.



Now to create your letter, highlight one the extension lines you had created in APCM, and press **Letter**. A Letter Attachment box will pop up and your letter will open.



When the letter opens, please amend / verify the following:

- Ensure that the address is correct, and its components are in the correct order:
  - Full name
    Street address, Apt. #
    City, Province (QC) postal code
    (REMOVE "CANADA" at the end of address)

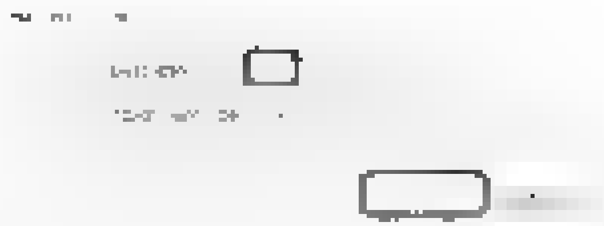
- Ensure that Mr. or Ms. is before the last name. However, if you are unsure of their gender, write their full name instead.
  - ie. Dear Mr. / Ms. Smith
  - ie. Dear Ashley Smith

- Remove the privacy brackets in the request text

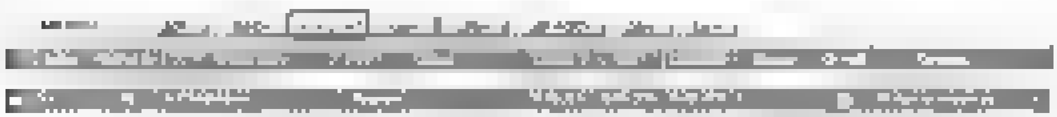
- Verify that the correct Team Leader's name (that will sign) appears at the bottom, and remove the second language (if the letter is English only keep the English title and so forth)

- Remove the cc to the Office of the Information Commissioner if it is not applicable (if it is an extension of 30 days or less).

Once completed, press save and then close the letter. You will now see a Letter Attachment pop up, type "letter" in the description and press **Attach**. The letter that you created will now be attached to your action. Only one letter is needed to be attached to an extension action (if you have more then one extension line)



If at any time you want to edit the letter, click on the action line in APCM, and press **Attachment**. Once your Attachment box opens, click on the letter and press Edit.



Always make sure that your letters look professional! CBSA has a letter standard. If you ever need to do modifications to your letter, please ensure that the presentation falls within these parameters.

Once your extension letter is done and saved, notify your Team Leader by email that the letter is ready to be signed. Once they have signed it, they will place it in the Mail-Out folder and create the mail-out action in APCM for the administration team.

<u>Team Leaders</u>: Steps on how to sign a letter electronically can be found in the chapter <u>Signing a Letter Electronically</u>.

17.2 Standard Extension Times for Certain OGDs

The following is a list of OGDs that have confirmed processing times that require us to claim extensions longer than 30 days under 9(1)(b).

OGD	Length	Rational
Department of National Defense (DND)		45 pages – 30 days 46-100 pages – 60 days 101-200 pages – 90 days 201-300 pages – 120 days

		300+ pages contact DND @ (613) 995 4344 **Files dealing with current operational material or major projects an additional 30 days should be added
Fisheries and Oceans Canada (DFO)		1-50 pages 30 days 51-150 pages 60 days 151-250 pages 90 days 250+ pages contact DFO by email at ATIP-LAIPRPCONCR@dfo-mpo.gc.ca
Global Affairs Canada (formerly DFAIT)	05-115 days	DFAIT requires 90 days for <50 pages and 120 days for >50 pages. Additional time is required in order to ensure transmittal and review of recommendations. Note: Analysts should contact DFAIT ATIP each time to confirm the processing time as it can vary depending on volume.
Public Services and Procurement Canada (formerly PWGSC)		1-50 pages 30 days 51-100 pages 60 days 101-200 pages 90 days 201-300 pages 120 days 400+ pages contact the receptionist at (873) 469-3648 who will redirect your call to the appropriate Operations Manager. *If you have an urgent file, timelines can be discussed on a case by case basis.
Royal Canadian Mounted Police (RCMP)		10 pages 30 days 00 pages 60 days 101-300 pages 90 days 301+ pages contact RCMP's ATIP Office at ATIP@rcmp-grc.gc.ca.

	*Documents of a complex nature and/or requiring consultation with multiple subject matter experts may require additional time **The day count starts on the date of receipt (date stamp) at RCMP
Sûreté du Québec	Analysts should contact their ATIP general mailbox at: accesdocuments@surete.qc.ca to obtain an estimated turnaround time. They will respond to emails within 24 hours. Please ensure to respect the timeframes provided by the Sûreté du Québec when completing your consults. Additionally, if providing a courtesy copy prior to the release of the information, please allow 5 business days. Any deviation to this, for any reason, must be approved by Dan Proulx
Transport Canada (TC)	1-25 pages – 60 days 26-100 pages – 90 days 101-200 pages – 120 days 200+ pages contact TC ATIP @ (613) 993-6162 or ATIP/AIPRP@tc.gc.ca

18. SENDING CONSULATIONS

The types of consultations are as follows:

18.1 Internal Review

CONSULTopi

CONSULTindividual

Legal Advice Sought

OPIReleaseCopy

Consultations within the Agency may be required when records retrieved from one sector contain information that originates from or concerns another sector, and the implicated sector was either not tasked with the retrieval, or if tasked did not provide the records in question.

18.2 OGD Consultations

CONSULTfederalDept

ATIP must consult with other government institutions if records that originate or pertain to those institutions form part of the material gathered in the response to the request. All consultations must be conducted within the statutory time frames set out in the ATIA. It is therefore important that OPIs flag any documents that they are providing to ATIP which may fall within this category so that consultations can be sent out as quickly as possible.

18.3 Cabinet Confidences

CONSULT – CABINETConfidence

18.3.1 Consultation with DLSU on the applicability of Cabinet Confidences

The Privy Council Office (PCO), in collaboration with the Treasury Board Secretariat (TBS) and the Department of Justice (DOJ), has revised the Cabinet confidences process to make it more efficient and reduce delays.

As of July 1, 2013, where a potential Cabinet confidence is identified by the Access to Information and Privacy (ATIP) Division, the ATIP Division will no longer consult with PCO via its Departmental Legal Services Unit (DLSU). Instead, the DLSU will process the consultation

and provide advice directly to ATIP. Only in complex cases and cases involving the "discussion paper" exception will DLSU consult with the PCO.

10.3.2 Cabinet Confidences – Section 69

CONSULT – CABINET Confidence

All Confidences of Cabinet are classified as Secret or higher. As such, any document that contain information that could be a Confidence of Cabinet must be processed on paper or on our stand alone Secret computer.

In accordance with Section 69, the ATIA does not apply to confidences of the Queen's Privy Council of Canada, which include:

- Memoranda presenting proposals or recommendations to Council;
- Discussion papers presenting background explanations, analysis of problems, or policy options to Council for consideration in making decisions;
- Agenda of Council or records indicating deliberations or decisions of Council;
- Records used for or reflecting communications or discussions between ministers of the Crown on matters relating to the making of government decisions or the formulation of government policy;
- Records briefing ministers of the Crown in matters before, or proposed to be brought before, Council;
- Draft legislation; and,
- Records that contain information about the contents of the types of records described above.

Note: "Council" means the Queen's Privy Council of Canada, committees of the Privy Council, Cabinet, and Cabinet committees.

There are instances, however, where even though the documents fall under one of the types described above, cannot be excluded as Confidences. These documents must be reviewed for possible release under the ATIA:

- Confidences of the Queen's Privy Council that are more than 20 years old;
- Discussion papers if the related decisions have been made public; or
- Where decisions have not been made public but four years have passed since the decisions were made.

10.4 Other Consultations

CONSULT province/municipality/police

ATIP must also consult with provincial and municipal governments as well as police departments when any records originating or pertaining to those institutions form part of the material.

gathered in response to the request. All consultations must be conducted within the statutory time frames set out in the ATIA or PA (many of these types of consults are found in PA requests as well). It is therefore important that OPIs flag any documents that they are providing to ATIP which may fall within this category so that consultations can be sent out as quickly as possible.

CONSULT ThirdParty

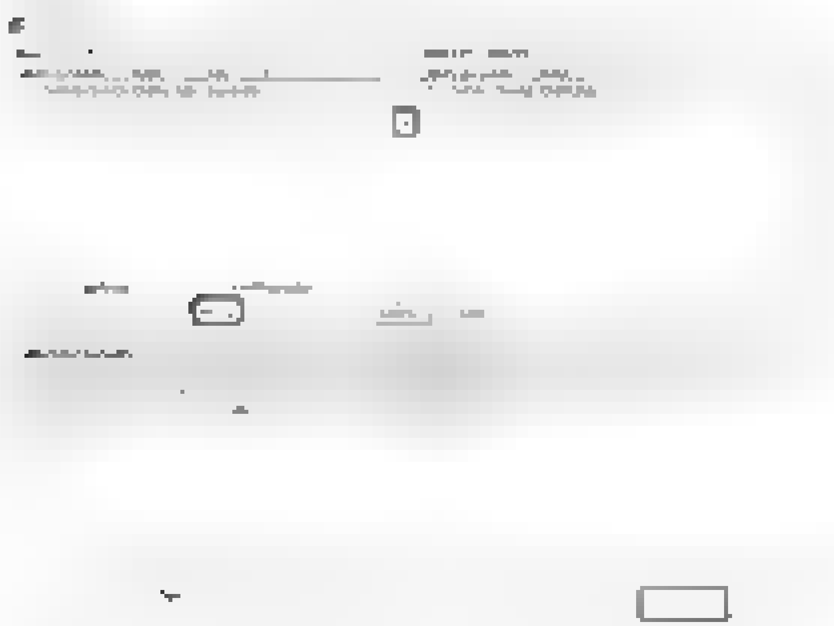
A "third party" is defined in section 3 of the ATIA as "any person, group of persons or organization other than the person that made the request or a government institution".

When dealing with records involving third parties, if the head of a government institution intends to disclose information that may contain information described in subsection 20(1) of the ATIA, they are required to notify the third party of this and allow them to provide representations as to why the information must be protected. If the institution intends to claim an exemption under section 20, the requirement for a notification pursuant to subsection 27(1) no longer applies. Please consult with your Team Leader if you are not sure of the need to consult or apply the exemption.

18.6 Creating a Consultation in APOM

If consultations are required on your file, your first step is to mark the records in Redaction for consultation. To do this, right click on the chosen page in redaction and select Consult.

A Consultation box will now appear. Use the **Search** feature to find the unit / organization that would you like to consult. Once you have found the unit / organization, double-click on them and it will bring the selection up to the top left. Next use > to bring the selection to the right hand side and then press **Save**.



Continue repeating these steps until all pages have been marked as Consult to the right unit / organization. Anyone that you have already marked to be consulted with on the file should already be in the top left box, so you can just press > to bring it to the right hand side and **Save**. To speed things up, you can use the CTRL or SHIFT key to make multiple page selections before you right click. Once this is completed, you will export the consultation package(s).

To create a consultation package in Redaction, use the drop down menu Request and select **Create Consultation Package**.

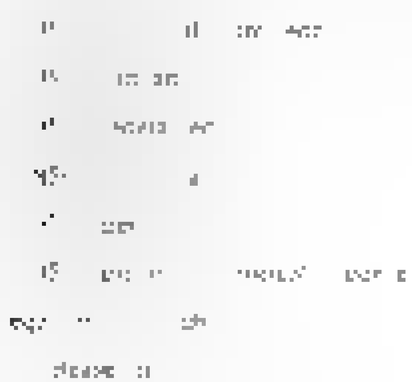
The units / organizations that you selected will be presented as options in this window, along with the number of pages you had marked for each. If you have consulted with multiple units/organizations, you will have to select and export each package individually. Select the one that you would like to start with, and press **Export**.

An Export / Print window will now pop-up. Choose Type: **PDF Format**, and check-off **Export/Print Original** and then select **Export**. Note: It is helpful to have a Save location on your desktop that you can regularly purge.

Once the export is complete, a consultation package in the form of a PDF will be produced and will pop up on your screen. Do a quality check on this consultation package. The consultation package will automatically be saved on your desktop. For more information on how to create a your location, refer to Exporting Your Release Package.

Note: If your consultation is internal, you do not need a consultation letter. You can simply save your consultation package on Apollo under the appropriate file number, and reference the location in which you placed the records in your email to the OPI. To do this, click on on the Consultation line in APCM and press the **Email** button.

If your consultation is external, you will need to create a consultation letter. To do this, click Add Action in your APCM screen, and select **Consultation**. The following options will be available to you, select the relevant option:

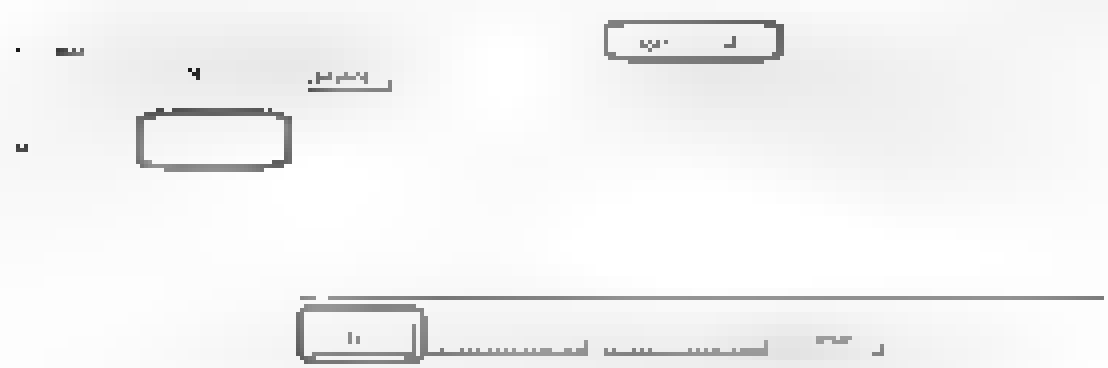


Once you have made your selection on the type of consultation and the Add Action box pops-up, the contacts that you've marked for consultation should automatically appear in the contact box.

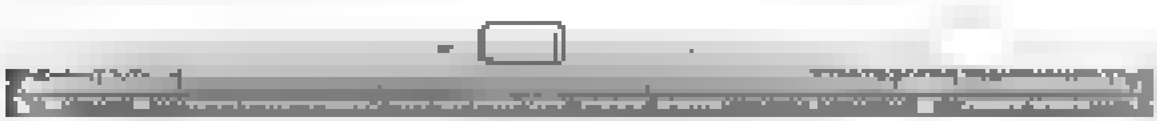
If you are still having issues with locating a contact, refer to this page for a list of all the Federal ATIP coordinators: http://www.tbs-sct.gc.ca/atip-aiprp/apps/coords/index-eng.asp

There is also a list of all the consultation contacts in APCM located here: Consult_Contact_List which is in the lists folder of the Employee Tools and References.

Once you have selected the contact, click on the selection and press > to bring it over to the right hand side. Leave "Date Completed" blank until you receive a final response from the contact. It is good practice to record the number of pages in the "Comment field" ie: 2 pages for consult. Once finished, press **Save**.



In APCM, click on the consultation line that you have created, and press **Letter**.



When the letter opens, please amend / verify the following:

- Ensure that the address is correct, and its components in the correct order:
  - Full name
  - Street address, Apt. #
  - City, Province (QC), postal code
  - (REMOVE "CANADA" at the end of address)

- Ensure that Mr. or Ms. is before the last name. However, if you are unsure of their gender, write their full name instead.
  - Ie: Dear Mr. / Ms. Smith
  - Ie: Dear Ashley Smith

- Remove the privacy brackets in the request text ( )

- Your name should be at the bottom of the letter (you will add your electronic signature). You can remove the second language (if the letter is English only keep the English title and vice versa).

- Indicate the number of pages in the "The attached ___ page(s) was / were" and edit the sentence so that it reads correctly. Ie. "The attached 2 pages were" or "The attached 1 page was".

- If it is not a True Access file, keep the sentence "For your information, we are in possession of the appropriate consent(s) necessary for the disclosure of the information". Remove the "(s)" if it involves the consent of only one individual or remove the "( )" if it involves more than one person's consent.

- For enclosure, indicate how many pages are being consulted. Ie. "2 pages for consultation"

Click on **File**, then **Print**, change your printer to Adobe PDF and then press **Print**. Save your letter on your computer.

Steps on how to sign your letter electronically can be found in the chapter Signing a Letter Electronically.

Once the letter has been completed, press **Save** and close it by pressing X to close the window. You will now see the Letter Attachment pop-up. Type "letter" in the description and press **Attach**. The letter that you created will now be attached to your action.

Create a folder specific to your request on your Desktop and use the following naming convention to name the folder:

- CON – FILE NUMBER – INITIAL

ON JL 2018 [illegible]

Next, place the Consultation Package and Response letter that you have already created in your desktop folder, and drag and drop (or cut and paste it) the folder into the Mail-out folder. Consultations should always be placed into the <u>MAIL TODAY</u> folder.

19. MANAGING SECRET RECORDS

Please follow the below procedures when processing all SECRET records. All SECRET records must be stored in the SECRET cabinets in the secret room when you are not working on them.

19.1 Receiving SECRET Records

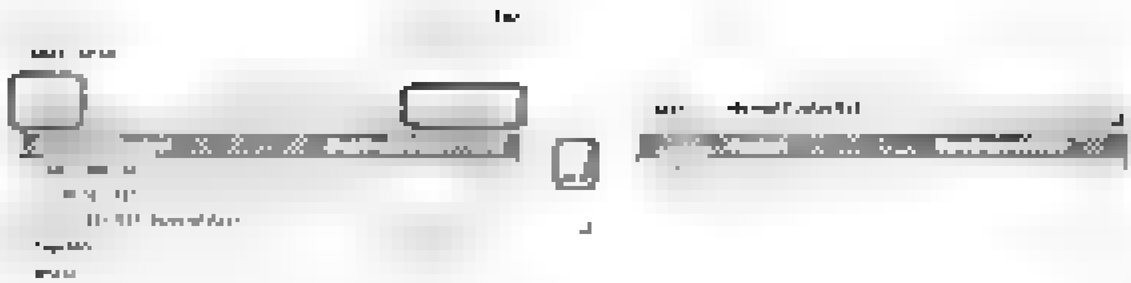
Once SECRET records are received, input the **Doc Type (h):** action to record that there are SECRET records on the file.

DocType (h):

To do this, go to Add Action, H – **Processing** and select **DocType (h).**

In the **Add** Action box, type "h" into the Name field and press **Search**. Select **h: SECRET** and press > to bring it over to the right hand side.

It is good practice to indicate the number of SECRET pages and their source in the Comment field. Leave the Date Completed blank and press **Save**. This Doc Type (h): action item will be closed <u>when the file is closed.</u>

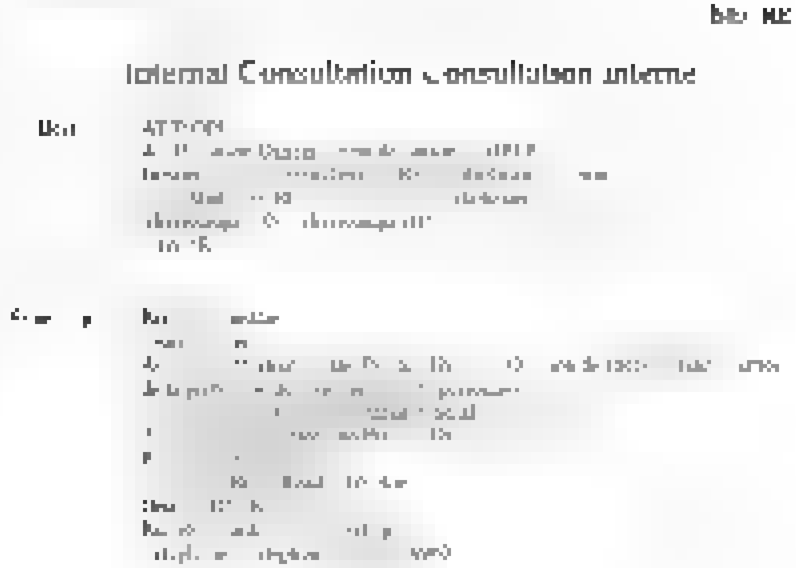


Retrieve a SECRET file docket (you can find these in the supply room) and write the file number on it. This docket will hold the records. When not in use, put this red folder – containing the secret records – in the secret cabinet in an individual hanging folder. The files are stored in numerical order in the cabinets without consideration to the file type (A, P, AC, PR, etc.). A-2018-12345 would go after P-2018-12344.

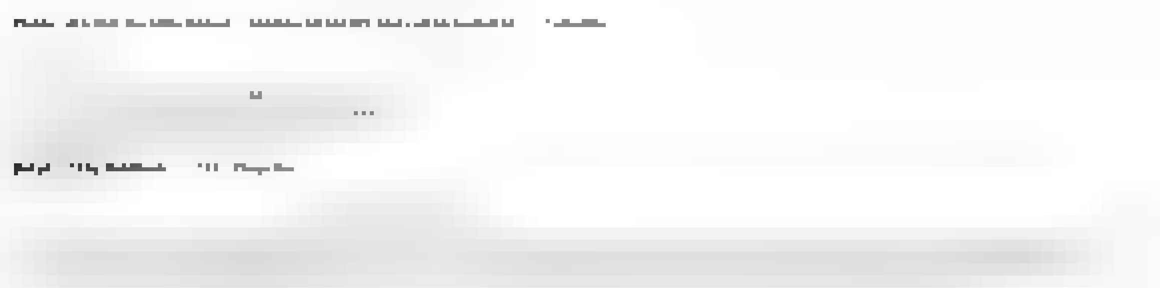
Please use the standalone printer in the Secret Room for all photocopies involving SECRET records.

19.2 Consulting SECRET Records

If you need to send a SECRET document for consultation, you will need to make a copy of the original documents. Always keep the originals clean, intact, and in our office. Make sure that your cover letter/memo is marked as SECRET on the top right corner. Place the letter/memo and the copies that you are sending in a new red secret folder for mail out.



Next, create a consult action in APCM and send an email to the OPI to inform them that SECRET records are being mailed to their attention.



19.3 Reviewing SECRET Records

Once you are ready to review your SECRET records, scan them into a standalone SecNet computer in the SECRET room. These computers are not attached to our network and are safe to use for SECRET records.

On the SecNet computer, you will use Adobe Acrobat Pro to mark your redactions. On the G drive of the SecNet computer, create a folder with your name (if you don't already have one), and then create a file folder titled with your file number (ie. A-2018-12345).

Scan in your records and place them in that folder. Create a second copy of your records naming the original copy your file number_ORG (ie. A-2018-12345_ORG.pdf) and the other

number_WC (ie. A-2018-12345_WC.pdf). The second copy will become the working copy. Never work with your original in case something happens to the file while vetting. Make sure that the original remains intact to avoid having to go back to the OPI for the records again.

Scan in all consults, recommendations and routing slips pertaining to the [illegible] request into the folder. Title them with names to indicate the owners of the documents (ie. A-2018-12345_Ops, RS and REC).

Double click on the working copy file, and Adobe Acrobat Pro will load. Record all recommendations received from the OPIs on your working copy, as well as your own by using the highlighter. The highlighter can be found at the top of the screen, in the toolbar.

If you want to change the colour of your highlighter to record your OPI recommendations, click on the text you have already highlighted, and go to Properties. For simplicity, use the yellow highlighter and add sticky notes to indicate what recommendations belong to which region, and under what section of the Act the severance should be made.

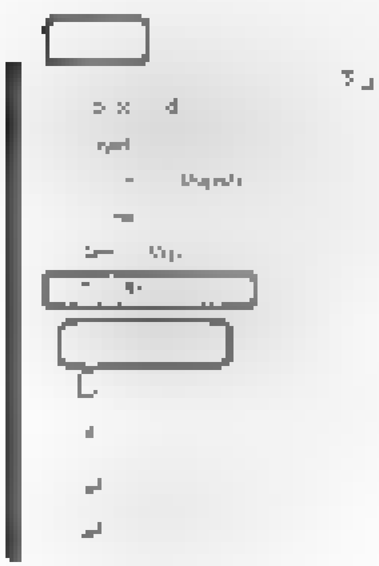
To add sticky notes, click on the bubble button left of the highlighter, and then double click on the highlighted text. A sticky note will appear.

Click on the top right to close the sticky note once you have inputted your text.

If the note is closed and you would like to edit it use the pointer arrow on your menu bar and click on the highlight again

Note: Documents must be OCR'd before you can vet documents in Adobe. If you get the following screen, click OK and the document will be automatically OCR'd for you

If you don't get the above window and are still having issues, manually OCR the document by going in the text recognition tab and click the In This File button



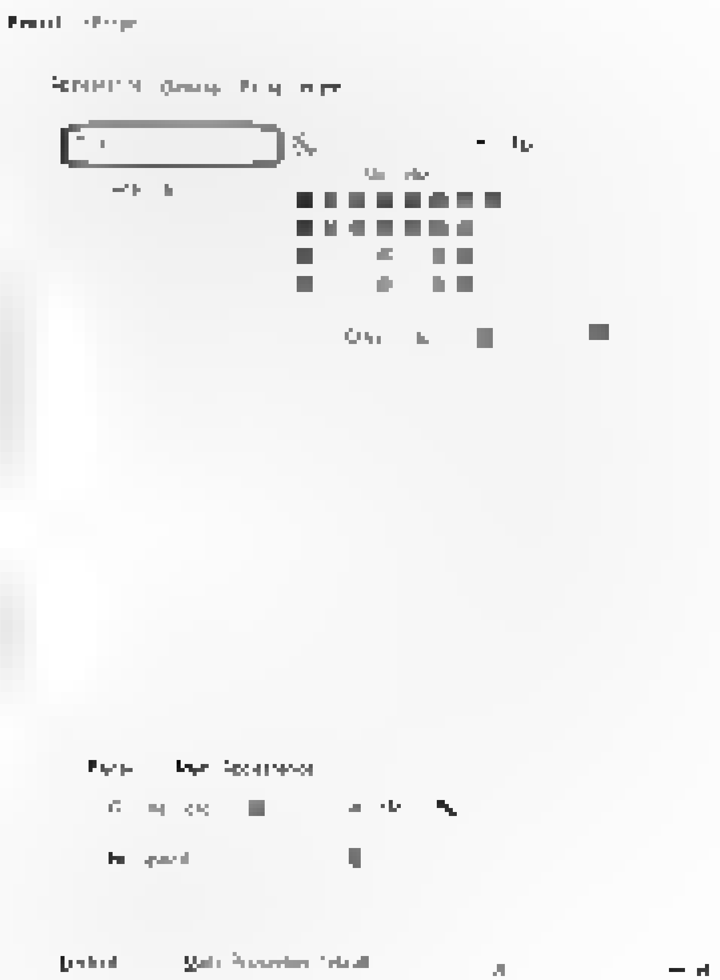
Once a file is OCR'd, you can highlight and vet the records

19.4 Preparing SECRET Records for Approval

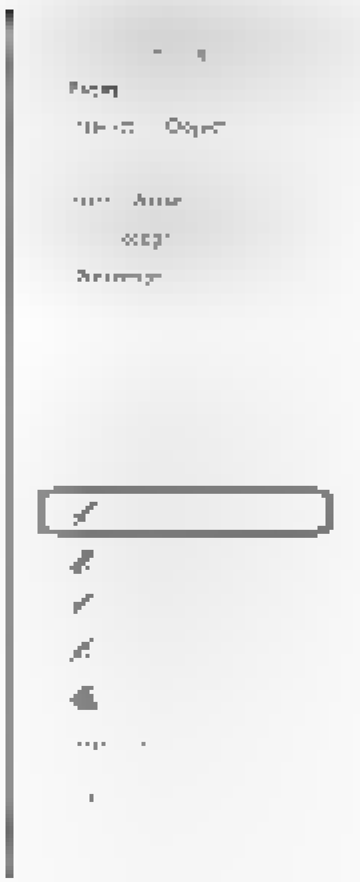
Once all of the recommendations are recorded in your working copy, it is ready for approval. The working copy should show all recommendations received, as well as your proposed severances. It will be the file that is reviewed by the decision maker. When the decision maker reviews the records they will use the same highlighting scheme as in redaction (turquoise for Assistant Directors and green for the Team Leaders).

Open the file and click on **Tools** on the top right of your screen to access your content editing options

Next, click on **Redaction Properties** in that menu and change the Redacted Area Fill Color to "no color". And press **OK**.



In your Tools menu, click on **Mark For Redaction**, and mark over all of the highlights. This will create a Red Frame around the text indicating that it will be redacted.



If you had highlighted or boxed something in error, place your cursor over the area, right click, and click delete. This will remove the highlight / red frame. You can also right click on notes to delete them as well.

Tip: Adobe's default cursor is meant to take out the text line by line. If you need to draw a box around an area that needs to be vetted, simply hold the CTRL key. It will change the cursor into a plus sign and allow for boxes to be drawn.

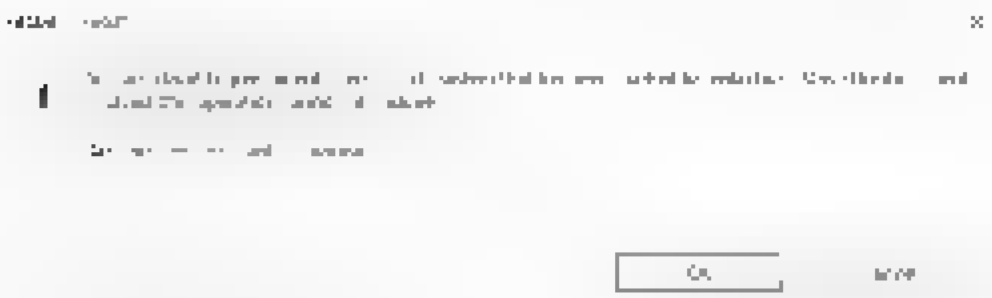
Lastly, before you submit your file for approval, change the SECRET action creation date to today's date (the day you submit it to your Team Leader/Assistant Director for approval). And place your red folder back in the SECRET filing cabinet.

19.6 Approved SECRET Records

Once your Team Leader/Assistant Director has finished reviewing, they will save a final copy titled as the file number_FINAL (ie. A-2018-12345_FINAL.pdf). The decision maker should be the only one to apply the redactions once they have approved the file. Once **Apply Redactions** is

pressed, the text is removed permanently. The only way to retrieve the text is to close the file without saving it and starting the file over.

When **Apply Redactions** is pressed, the following box will appear. Press **OK**.



Redactions will be applied, and you can press **Yes**.

If the above screen does not appear, and instead this screen appears

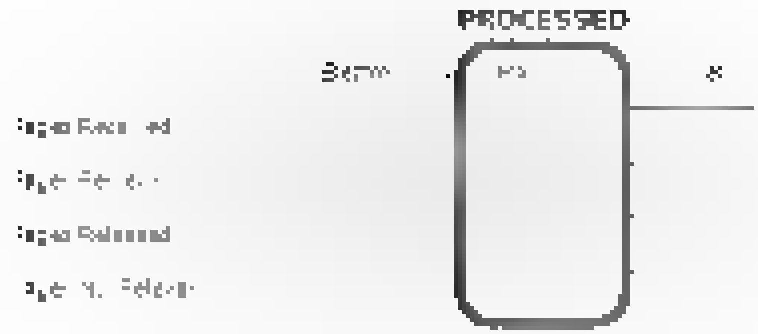
Click Remove when it is done scanning the document to ensure that any hidden information is removed from the file before providing it to the client. Make sure that all notes and highlights applied to the document are removed as well. Save the document.

Once finished, you will have 4 files:

- The original with nothing on the page – **A-2018-12345_Org**
- The Analyst processing file (OPI recommendations and Analyst severing, sticky notes etc. – **A-2018-12345_WC**
- OPIs routing slip and recommendations – **A-2018-12345_OPI RS and REC**
- The final disclosure that will be sent to the applicant – **A-2018-12345_Final**

When the SECRET records have been approved and severed, they are to be printed off the Secret computer and scanned into Redaction to be included with the rest of the files records. <u>Always do a quality check of these records when they come back from Approval.</u>

Please ensure that the pages withheld are recorded to ensure that the proper page count is accounted for. Manually record these pages in the closing screen.



Any/all exemptions/exclusions used also need to be manually entered in APCM. To do this, click on the **Exemptions** button in APCM. Select the sections of the Act used on the SECRET pages <u>if they were not already used in your file</u>. Press > and then Save.

Before sending to mail out, enter the Date Completed of the SECRET action to today's date. Put a note when closing the action (DD/MM initials) in Secret cabinet and move it to a different cabinet for closed files. Return the SECRET file to the SECRET room and place the SECRET documents in the SECRET cabinet for closed file.

20. RECORDING DELAYS AND LEVEL OF COMPLEXITY

20.1 Complexity (Access and Privacy files only)

For the annual report, the factors that increased the complexity our requests.

There are three types of complexities, and a request can have more than one type.

1. Consultation Required

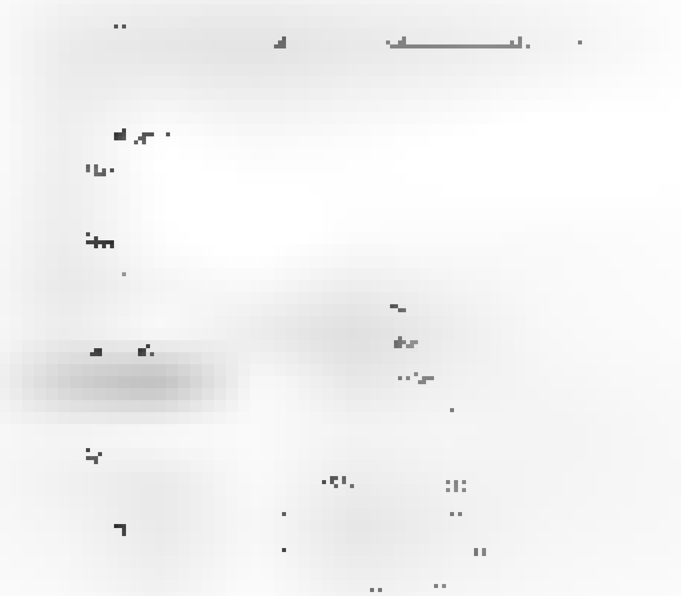
   This complexity type is found in requests that require consultations outside of the institution. When consultation actions are on a file, there are no additional steps required by the officer in order to flag. The system will automatically detect any consultation actions.

2. Legal Advice Sought

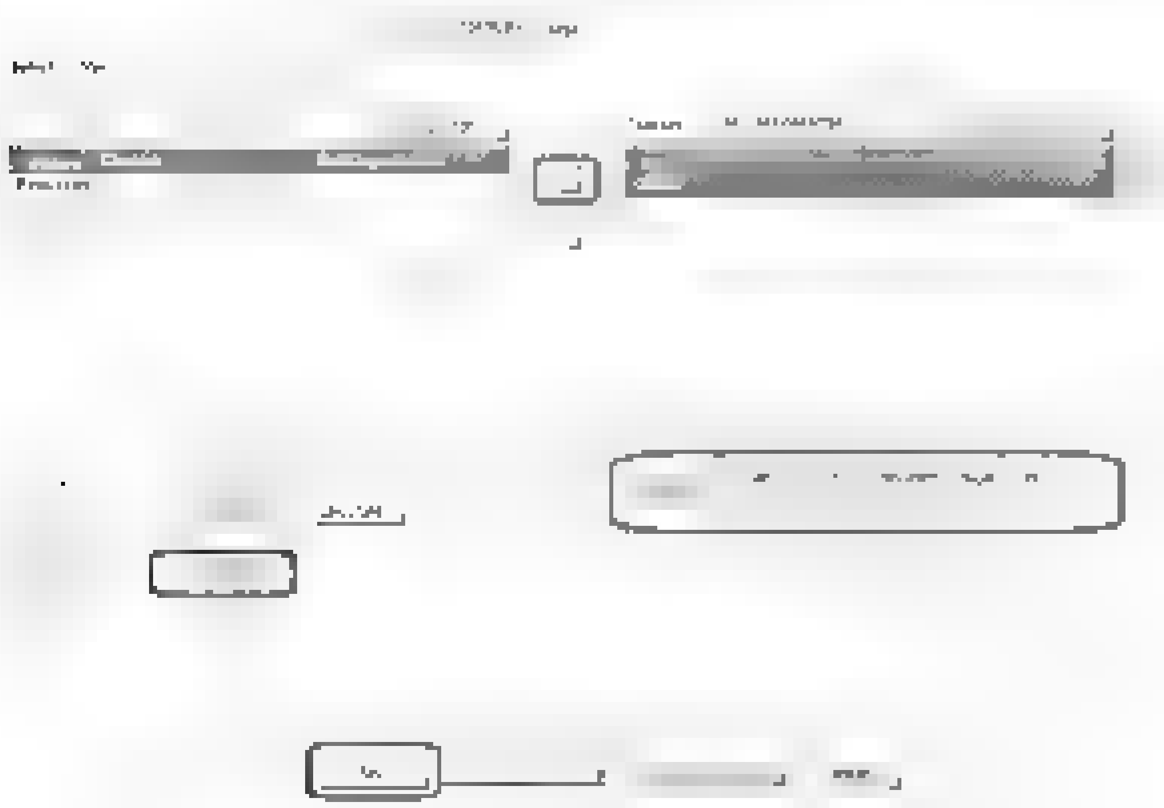
MANDATORY > COMPLEXITYLegal

This complexity type must only be used to report instances where the ATIP Office sought legal advice that was considered necessary in order to respond to a request. Consultations with legal services in order to consult with the Privy Council Office regarding the applicability of section 69 are not be included in this category.

To add the *COMPLEXITYLegal* flag, go to Add Action, **MANDATORY** and select **COMPLEXITYLegal**



Once in the **Add Action** box, click on **Officer** and then > to bring that selection to the right hand side. Add a note in the Comment field summarizing the reason for requesting a legal opinion, your initials and today's date. Then input today's date into Date Completed to close the action. Press **Save**.



3. <u>Other</u>

MANDATORY > *COMPLEXITYOther*

These files have other complexities relating to the processing of a request that are not addressed by the other complexity types (consultations or legal). Examples include: requests for the contents of a database, requests to process audio or video recordings, high profile subject matter, cases where records are in a region or other country, and cases where the records are in a language other than English or French.

To add this flag, follow the same instructions as above in *COMPLEXITYLegal*, with the exception of the comments field. For *COMPLEXITYOther*, you must describe the complexity of your file briefly in the comments field.

20.2 DELAY / DEEMED REFUSAL REASONS (Access and Privacy files only)

A delay reason action must be added to all late Access and Privacy files. This action allows us to quickly understand why the file was not completed in the legislative timeframe. Only <u>one</u> reason can be added to the file, so please pick the one that had the greatest impact.

There are 4 types of delay reasons:

1. <u>Workload</u>

MANDATORY > *DELAYREASONWorkload*

This reason is used when you have a large number of requests to be processed, very large requests or other ATIP-related tasks (e.g., complaints, training, PIAs, PIBs, Info Source, assessments under the Management Accountability Framework).

2. <u>External Consultation</u>

MANDATORY > *DELAYREASONExternalConsult*

This reason is used when your file has consultations with individuals or entities that are not part of the institution, including third parties and other government institutions. It also includes consultations with the Department of Justice legal counsel.

3. <u>Internal Consultation - Capacity</u>

MANDATORY > *DELAYREASONInternalConsult*

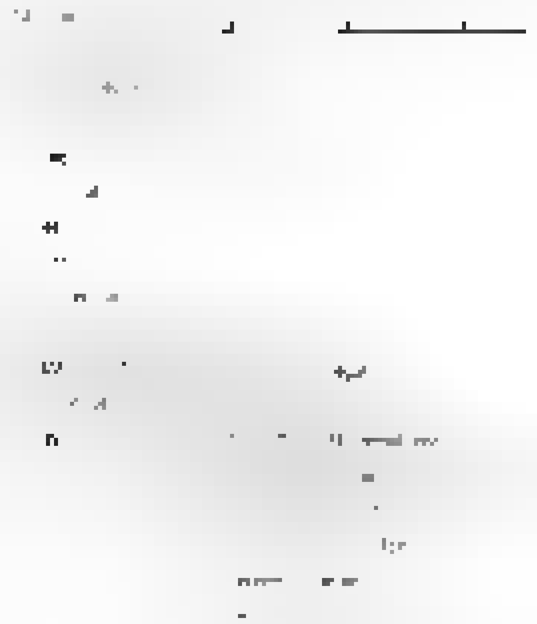
This reason is used when your file has consultations with officials within the institution, and/or consultants and legal agents working for the institution.

4. <u>Other</u>

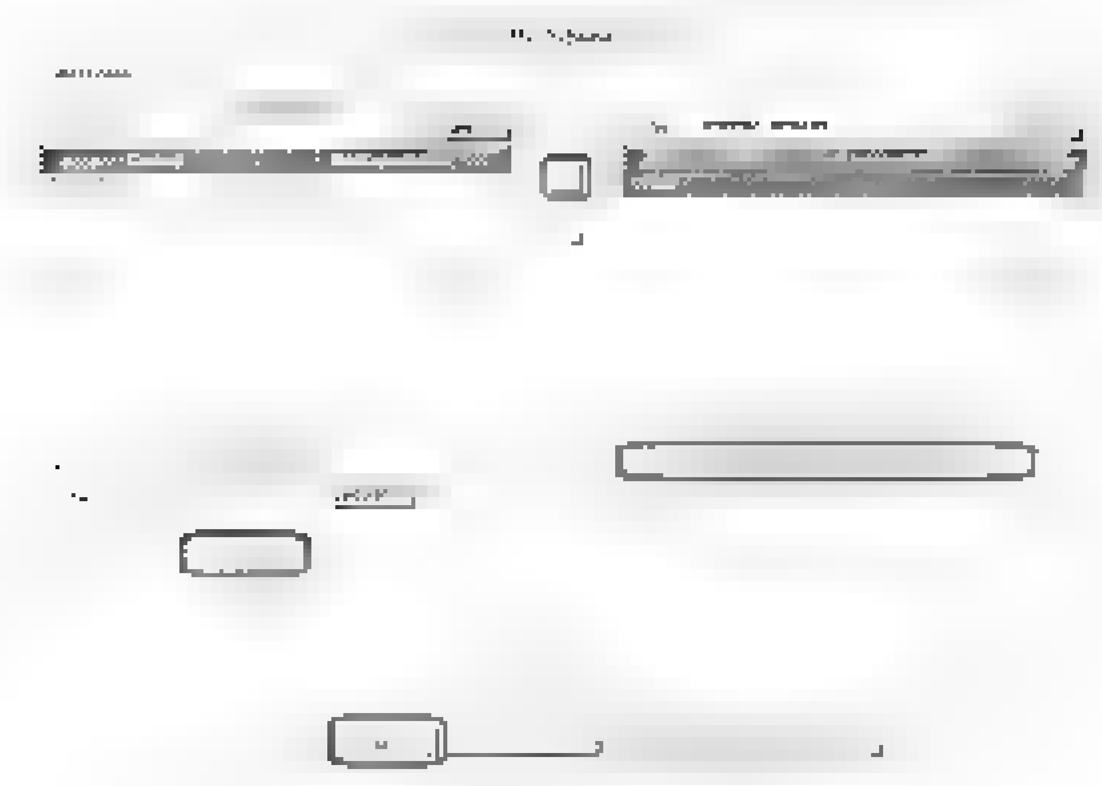
MANDATORY > *DELAYREASONOther*

This reason is to be used for instances other than workload and consultations (examples are: unavailability of key officials, difficulties in obtaining relevant records, labour disputes, and lengthy power outages).

To add a delay reason, go to Add Action > **MANDATORY** and select **the applicable delay reason**.



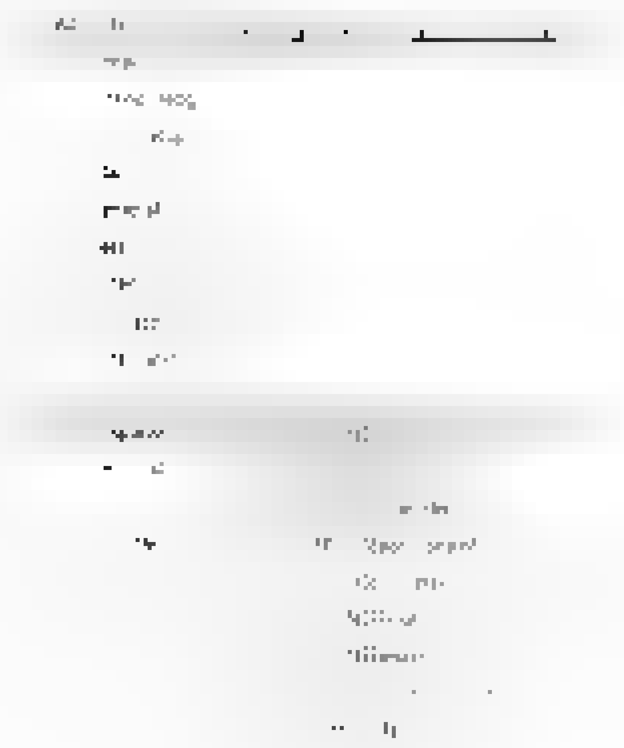
Once in the Add Action box, click on **Officer** and then > to bring the selection to the right hand side. Please add a note in the **Comment** field summarizing the delay, your initials and today's date, then input today's date into **Date Completed** to close the action. **Press Save.**



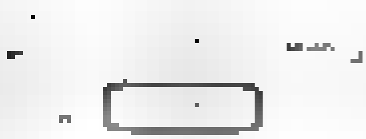
21 PREPARING YOUR RESPONSE LETTER

Once your file has been reviewed and is ready for approval, you are going to prepare your response letter. To do this, go to Add Action, select [illegible] **Response** and then **RESPONSE**.

Please note that if you are working on a Privacy request, Phase [illegible] Requests, Traveller History, or Consultation, they each have their own response letter. Each section related to these request contain specific instructions regarding the response letters.



Once your Add Action box pops up, enter the Date Completed as today's date, and click on Requester, then Save and Letter.



Your response letter will now appear. Ensure that the address is correct, and that its components in the correct order:

- Full name
- Street address, Apt. #
- City, Province (QC), postal code
- (REMOVE "CANADA" at the end of address)

Ensure that Mr. or Ms. is before the last name. If you are unsure of their gender, write their full name instead.

- ie. Dear Mr. / Ms. Smith
- ie. Dear Ashley Smith

Verify that the correct Team Leader's name (that will be approving your review) appears above Enclosure.

On the second page: Delete "Your Request Number" row if the requester did not have a file number. In the Request Summary, remove the privacy brackets.

If the disposition is "All disclosed" or "Does not exist", remove the sentence starting with "The following line indicates which section(s)…". Remove the statement "Summary of the exemptions…" in their entirety.

If the disposition is "Disclosed in part", modify the line "The following line indicates which section(s)…" by dropping the "s" or the () and remove either "was" or "were". Make sure that all exemptions are included in the Summary of the exemptions. If there are no exclusions, delete "Exclusions" in the text.

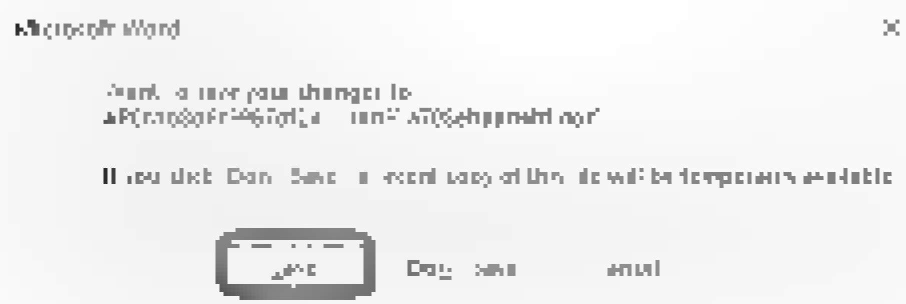
In the section Link to the Acts, remove the link that is not relevant to the request type (Access or Privacy request) and delete the other one.

Remove the Comments line if there were no comments to add.

For the Enclosure, it should read "Enclosure – A copy of the release package to the applicant".

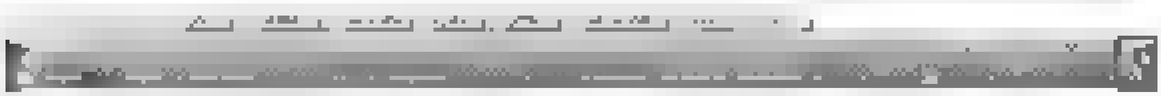
Always make sure that your letters look professional! CBSA has a letter standard. If you ever need to do modifications to your letter, please ensure that the presentation falls within these parameters.

Once you are done reviewing/modifying your letter, close it and you will be prompted to save. Press **Save**.



Next, a **Letter Attachment** box will appear. Type "letter" in Description, and press **Attach**.

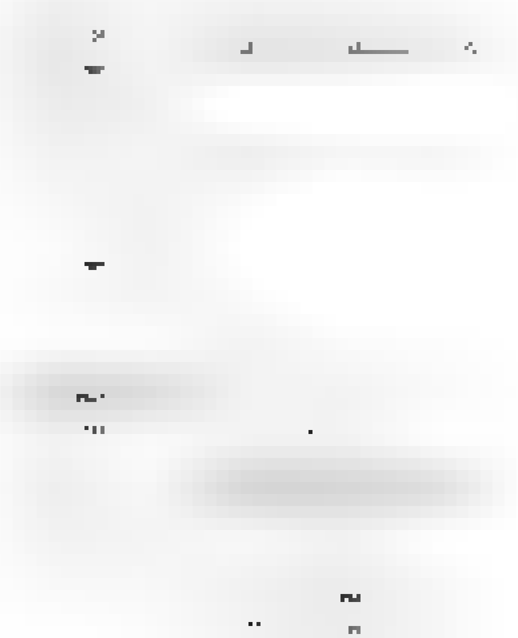
The attachment will now appear in the RESPONSE action in APCM. If you do need to access the response letter, or edit it, click on the RESPONSE line in APCM and press the **Attachment** button above.



21.1 Additional Records Response

If additional records are to be released on a file after the initial release, you will need to produce an additional records response letter.

In APCM, go to Add Action, select **IC – Response** and then **RESPONSEadditionalInfo.**



The next steps are the same as a regular response letter. Once your Add Action box pops up, you can enter the Date Completed as today's date, and click on **Requester**, then **Save and Letter**.

Once you have pressed **Save and Letter**, you will be prompted to select a template:

- **All Withheld** (in this case, the requester will only receive the letter indicating additional records were found, but are being withheld).
- **Full Release** (you will send sending them another release package)
- **Partial Release** (you will send sending them another release package)

Your response letter will now appear. Ensure that the address is correct and that its components are in the correct order:

- Full name
  Street address, Apt. #
  City, Province (QC) postal code
  (REMOVE "CANADA" at the end of address)

Ensure Mr. or Ms. is before the last name, however if you are unsure of their gender write their full name instead.

- ie: Dear Mr. / Ms. Smith
  ie: Dear Ashley Smith

Verify that the correct Team Leader's name (that will approve) appears above Enclosure.

Delete "Your File" if they did not have one. In the Request Summary, remove the privacy brackets.

If your additional records are either partially exempted or fully withheld, delete "exempted" or "excluded" from the text. Ensure that all sections of the Act are referenced. Delete the brackets (s) when only one section of the Act is referenced and do the same under Enclosures. In the letter you should include paper copies of the sections cited. The sections can be found here.

Try and get your letter to fit one page. If it is not possible, insert "…/2" at the bottom right of your first page and ensure "- 2 -" is at the top of your second page.

Once you are done modifying the letter, close it and you will be prompted to save. Press **Save**.

Next, a Letter Attachment box will appear; type "add_letter" in Description, and then press **Attach**.

The attachment will now appear in the RESPONSEAdditionalInfo action in APCM. If you do need to access it or edit it, click on the RESPONSE line in APCM and press the **Attachment** button above.

22. APPROVAL OF FILES

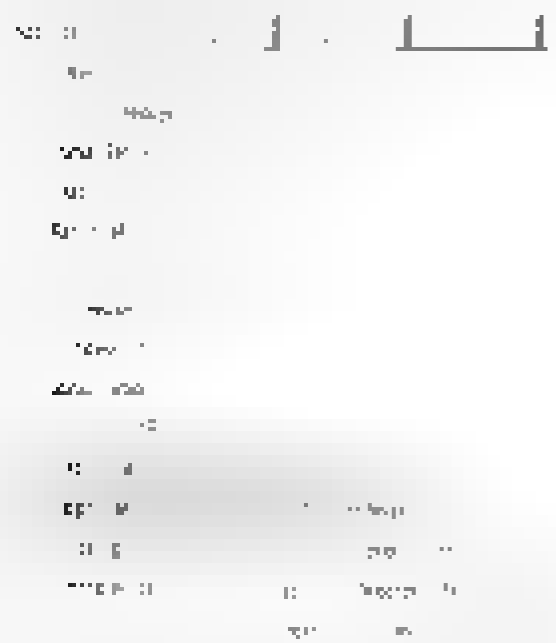
22.1 Approval and Signature Actions

Once an Analyst has completed the review of a file and is ready to have their Team Leader review the final product, they create an Approval and Signature action and place the file in their Team Leader's tree in APCM.

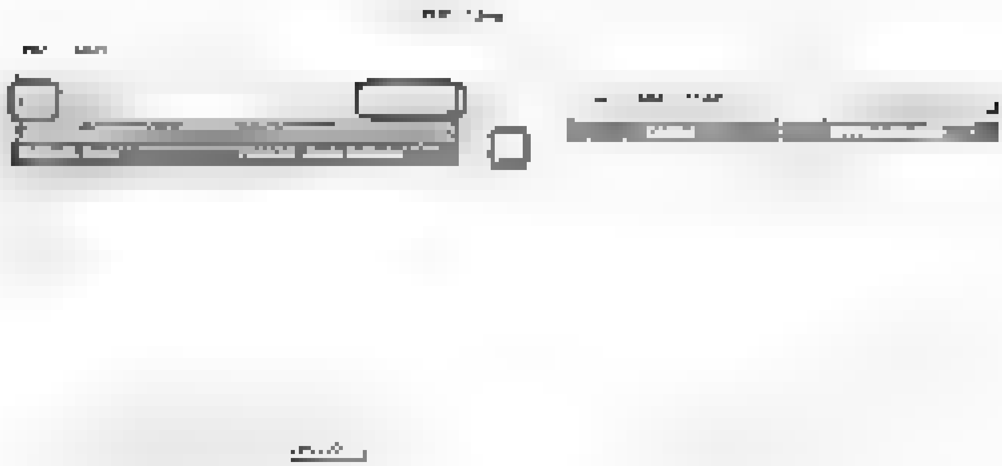
Approval/final

Signature

To create the approval action, click on **Add Action**, then **Approval** and lastly **APPROVAL/final**

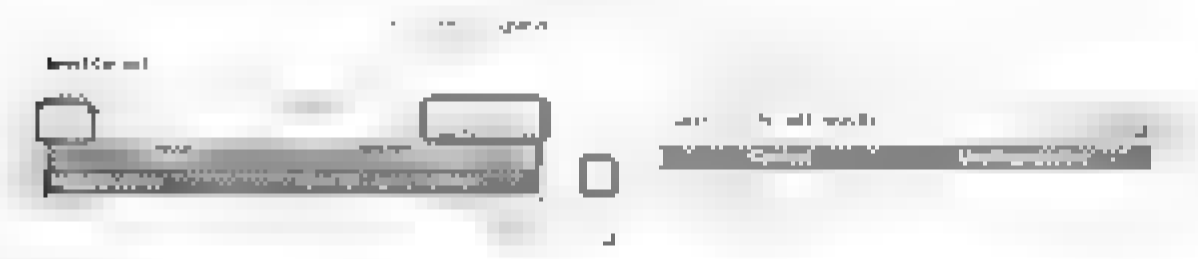


Once the Approval Action is open, type in the last name (or partial last name) in the **Name** field and then press **Search**. Once your Team Leader is found, click on their name to select it and then press > to bring it to the right hand side. Leave the Date completed open, and press **Save**.

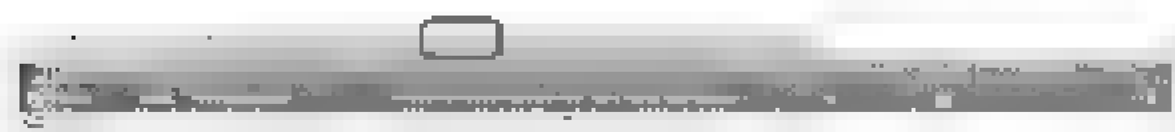


Next, to create the Signature action, click on **Add Action**, then **M**... Closing and lastly Signature

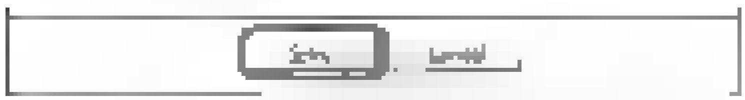
Once the **Signature Action** is open, type in the last name (or partial last name) in the **Name** field and then press **Search**. Once your team leader is found, click on their name to select it and then press > to bring it to the right. Leave the Date Completed open and press **Save**.



If the file is due that day, the Analyst should send an email to their Team Leader to notify them. You can do this by clicking on the Approval action line in APCM. Once it is highlighted, press **Email**.



A Select Template box will pop-up.

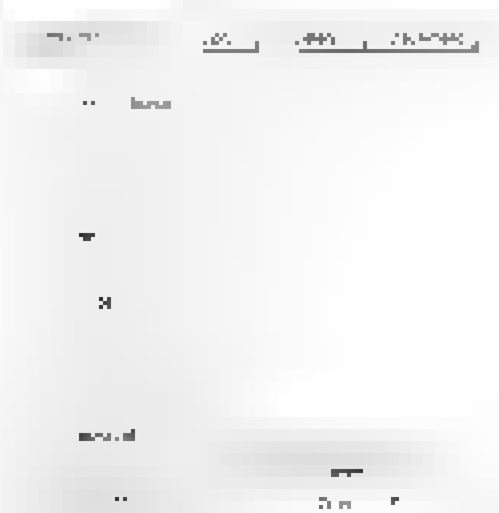


Click on **For Appr Due TODAY** and then **Select**. A template email will then pop up for you to send

22.2 Preliminary Approvals

APPROVAL preliminary

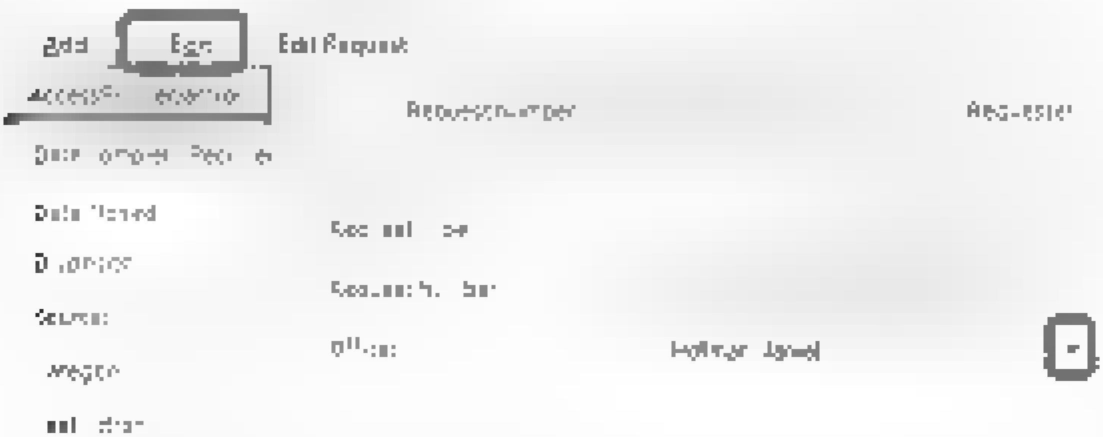
A preliminary review action can also be used when needed for complex files. In cases where you would like your Team Leader to review before your own review is complete. The steps are the same as an APPROVAL final with the exception of the action that you will choose instead (APPROVAL preliminary)



Once the Approval action has been added to your file, you may place it in your Team Leader's tree for their review. Your Team Leader will open your request and review the records, offering their advice on any changes that may be needed.

22.3 Transferring a File to your Team Leader

To transfer a file to your Team Leader for approval, click on the **Edit** button on your main APCM screen, and press the Arrow down beside officer to find your Team Leader's name. Once you find their name in the Officer field, select it and it will appear in their tree.

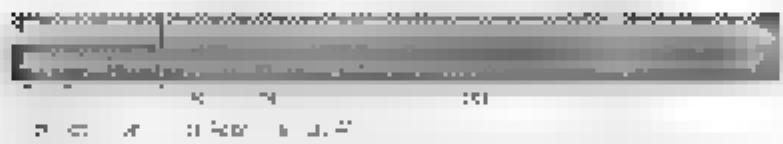


Once the TL has completed the review and is satisfied with the disclosure of the request, they will close the Approval action and the Signature action. Closing both actions simply involves the Team Leader double clicking on the action line in APCM and entering the Date Completed action as today's date. They may or may not include comments in the Comment field for the Analyst.

Team Leaders: Steps on how to sign a letter electronically can be found in the chapter Signing a Letter Electronically.

There are also emails available for the Team Leaders to notify the Analyst of the Approval being completed. To access these emails, the Team Leader can click on the APPROVAL final action in APCM and press **Email**. An **Approved – to Analyst** email and **File Returned to Analyst for Changes** email templates are available for use. To use them, click on the appropriate template and press **Select**.

Select Review



Once they finish their review, the TL will return the file back into your name (placing it back in your tray) for you to export your release package.

After the file has been returned by the Team Leader, the Analyst should review the file for any modifications made or required, in Redaction.

Note: For Travel History files, the Team Leader will place it back in your name, BUT place it in mail-out for you. You will not see this type of file returned to you, unless there are changes to be made in the file.

22.4 True Access Approvals

True Access requests have a few extra review steps.

22.4.1 Assistant Director / Director's Reviews

Assistant Director's Review

Director's Briefing – Review

True Access files require an Assistant Director Briefing, which is a meeting with your Assistant Director to go over your proposed release and any OPI recommendations. Afterwards, your Assistant Director will meet with the Executive Director to go over what releases are taking place within their teams.

Once the Final Access file is passed this stage, a copy of the release package is then placed on the shared drive for the Communications Directorate to review the material and prepare media lines (if needed).

22.4.2 Communications Review

HEADS UP Format to C+I

These action lines should also be set up on your file (Briefing Folder Copy and COMMUNICATIONS)

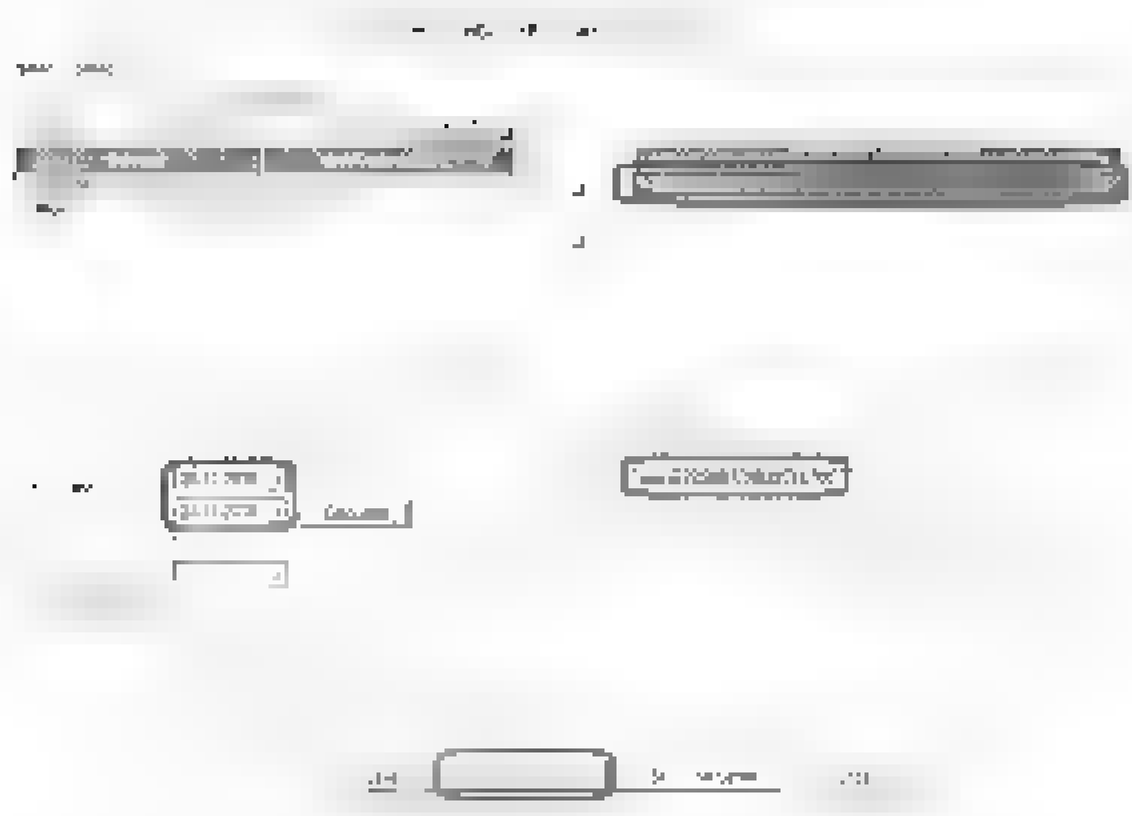
[illegible]

At this stage you need to export your release package to the following location:

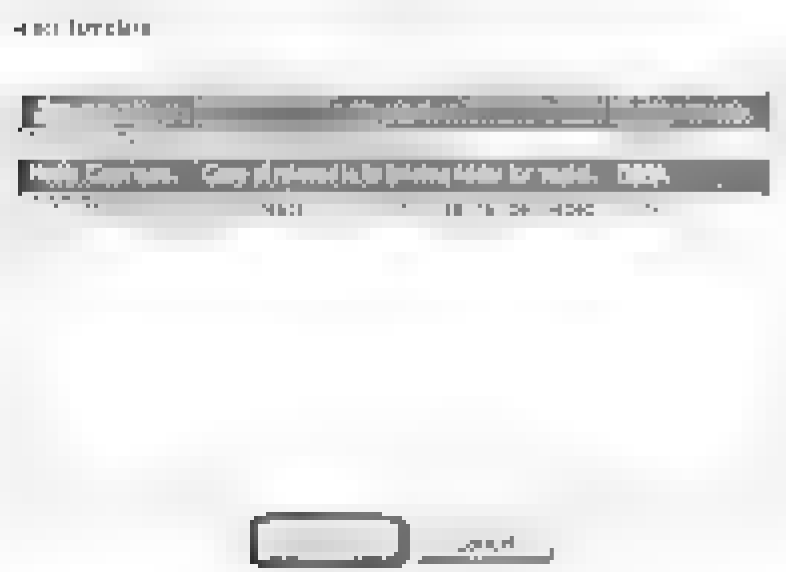
If your records are SECRET, contact Communications first to ensure that they need to review (mentioning the records are SECRET). If they wish to review, make a copy of your records (on the stand alone copier in the SECRET room) and send them over by courier. Be sure to create a Word Document in the Briefing Folder to indicate that the records are SECRET (example below) and cannot be saved on the shared drive.

Once your records (or Word Documents) are uploaded in the Briefing folder, you can close that action by double clicking on the HEADS-UP Format to (Briefing Folder Copy) action line and entering the **Date Completed** as the present date. Type in the **Comment:** field "uploaded" + today's date and your initials.

Next, send an email to Communications. To do this, open your HEADS-UP Format to (Communications) action in APCM. Change the **Date Created** to today's date, and press **Calculate**. It will automatically update the **Due Date** for you. Type in the **Comment:** field "sent to COMMS" + today's date and your initials. Click on **COMMUNICATIONS** above and then **Save And Email**.

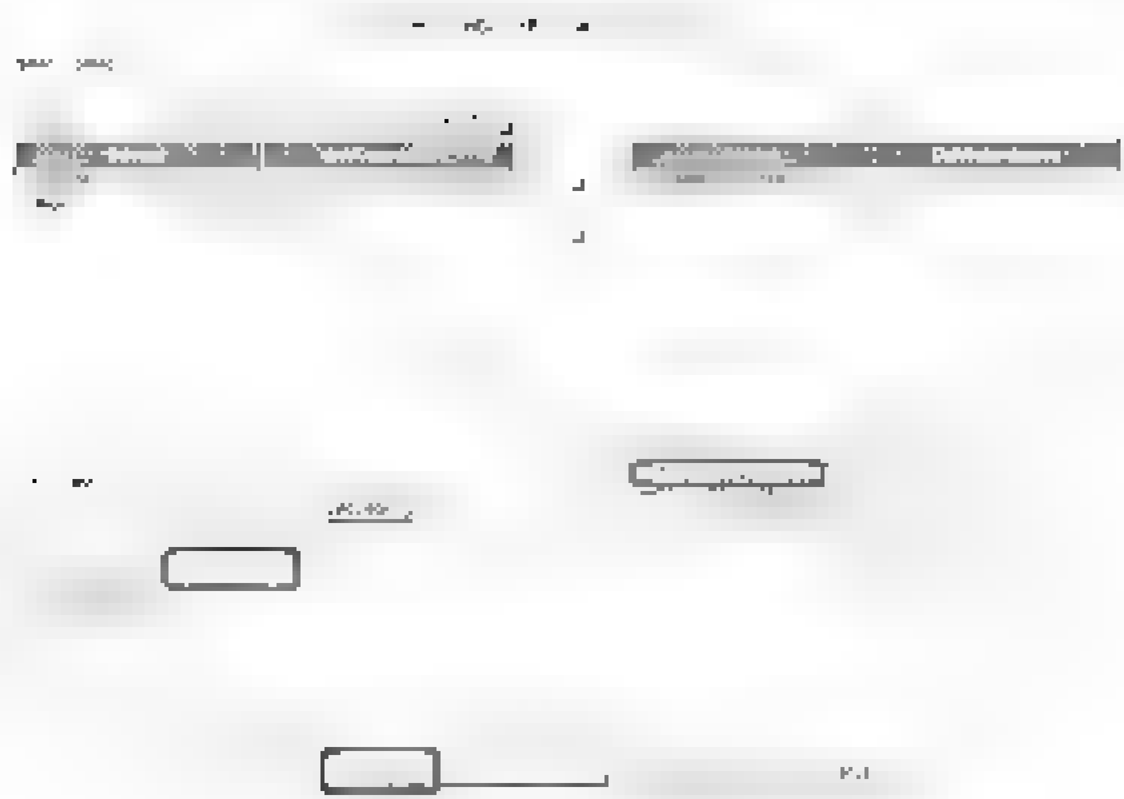


Template options will now pop up. Click on **Notify Communications** and press **Select**.



The red text below indicates where editing will be required. Indicate which OPI was tested, any special notes (if you are sending SECRET records by courier, indicate this here), and complete the drive name. If there are SECRET records, the drive name isn't necessary. Once complete press **Send**.

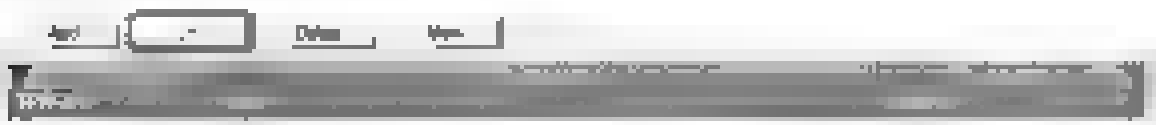
Once Communications has reviewed your release package, they will send you an email indicating that their review is complete. If they have any questions or concerns, they will express it in that email. Once Communications is satisfied, you may close the action in APCM by double clicking on the action line, writing COMMS ok (if that is the case) in the **Comment field**, entering the Date Completed as today, and lastly press **Save**.



23. SIGNING A LETTER ELECTRONICALLY

Analysts are to have created the response letter in APTM in Word Format. From there, the delegated officer will open the letter in APTM. To open the letter, click once on the action line and press the **Attachment** button.

Select the letter and press Edit.



There are two ways in which you can sign the response letter: through Adobe and with Word.

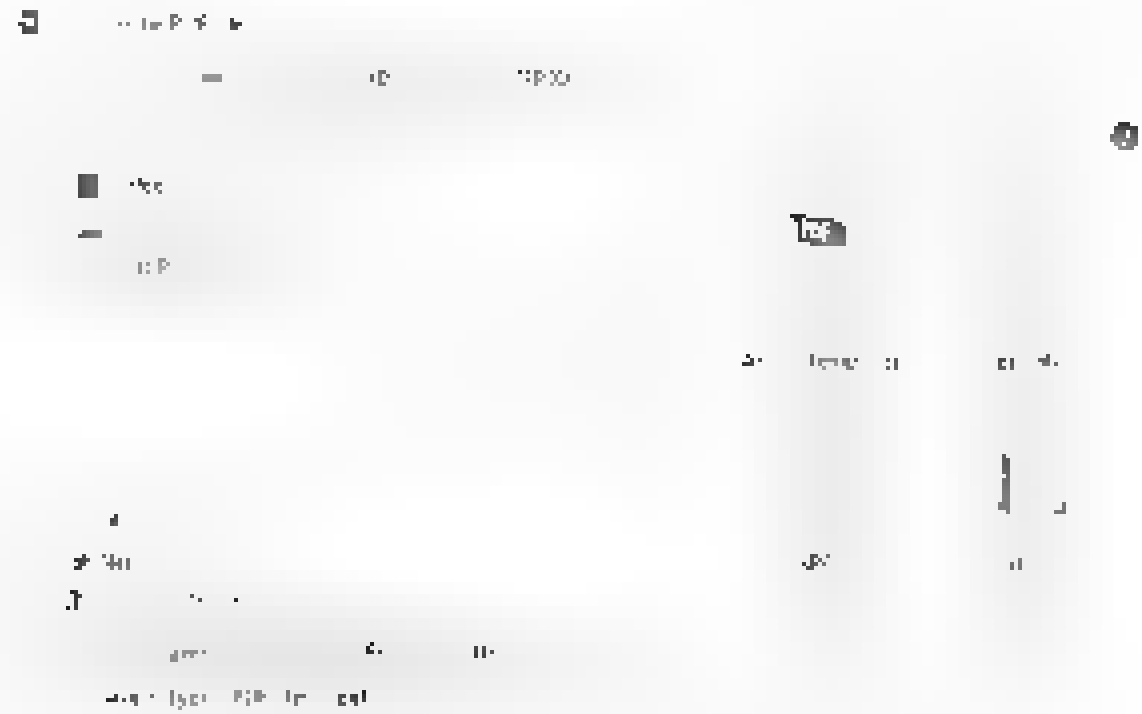
23.1 Signing a Letter using Adobe

Press Edit Attachment.

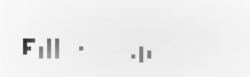
Always make sure that your letters look professional! CBSA has a letter standard. If you ever need to do modifications to your letter, please ensure that the presentation falls within these parameters.

Once the letter opens, press the **File** Tab and select **Save as PDF**

Save the letter as the File name – Response letter *.pdf* in a temporary file on your H: drive

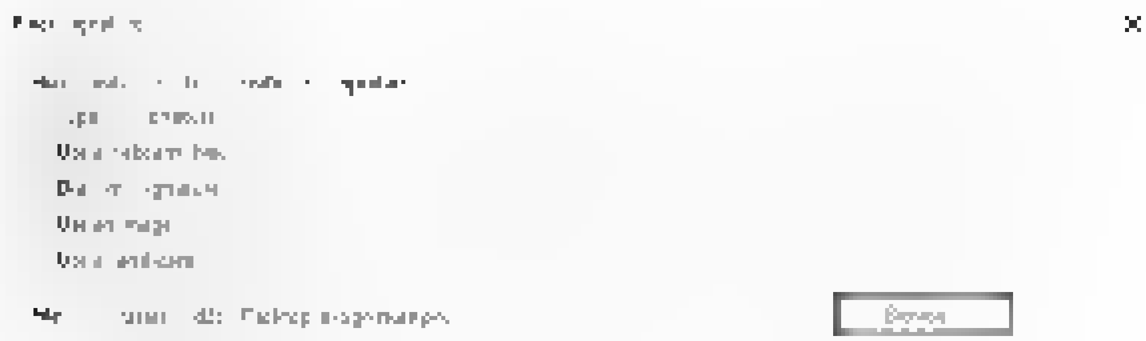


Once the PDF opens, press **Fill & Sign** at the top of the screen



One that tool box opens, select **Place Signature**

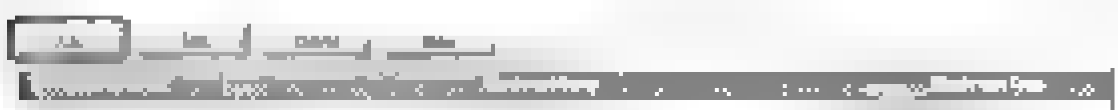
When the Place Signature box pops up, select **Use an image**. If you haven't yet done an e-signature, see the Operations Team to help you. They will scan an image of your signature for you to save on your desktop to use for your letters. Once have your e-signature, press **Browse** to retrieve it from your desktop. Once selected, press **Accept**.



Place your signature on your letter and press **Save** once completed. The file name will now have added "...signed" at the end.

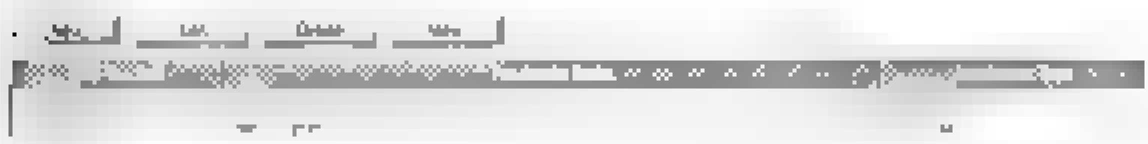
The Word document of the letter will still be open, you can close that window now. There is no need to save this copy. Press **Cancel**, at the Edit attachment window.

With your Attachment window still open, press **Add**.



Press Browse to find your signed letter in the temp file on your H: drive, and type "letter-signed" in your **Attachment Name** field and press **Save**.

You will now see both letters in the Attachment window. Press OK.



The letter is now ready for the Analyst to export for their mail-out.

22.1 Signing a Letter using Microsoft Word

Press Edit Attachment.

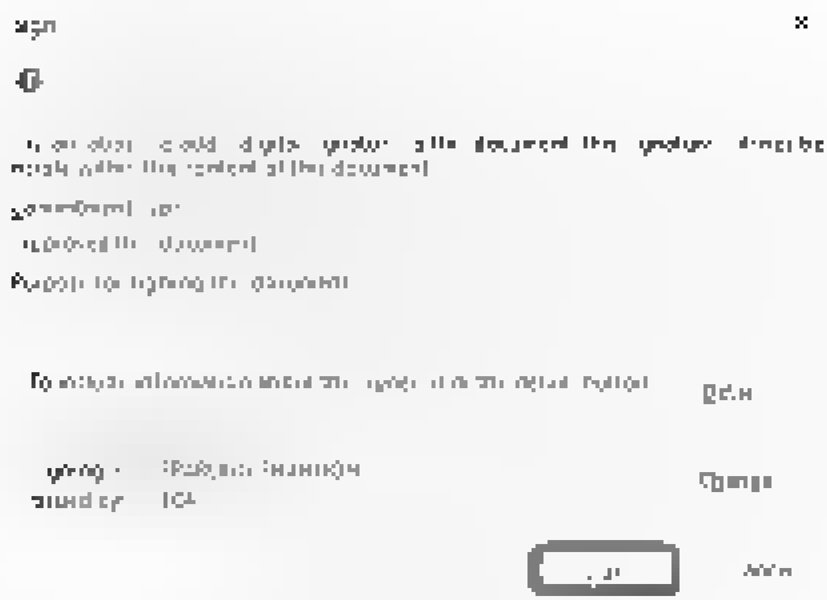
Always make sure that your letters look professional! CBSA has a letter standard. If you ever need to do modifications to your letter, please ensure that the presentation falls within these parameters.

Once the letter opens, paste or insert your e-signature into the appropriate place on your letter. If you haven't yet done an e-signature, see the Operations team to help you. They will scan an image of your signature for you to save on your desktop to use for your letters.

Go to the **File** menu tab and choose **Protect Document**.

Now select **Add a Digital Signature**.

A **Sign** box will now pop up, select the appropriate action in the **Commitment Type** box, and then press **Sign**.

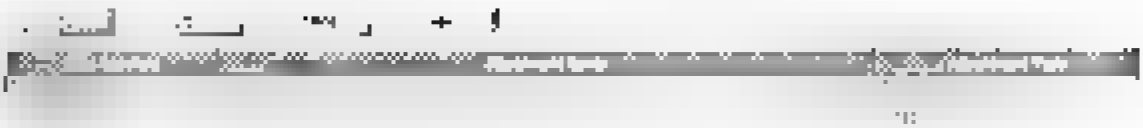


You will now be prompted for your Entrust password. Once you have entered your password, you will receive a Signature Confirmation. Press OK.

Your letter will be marked as Final. This is indicated by a yellow banner on the top of your screen. If someone wants to Edit the letter, your signature will be removed.

Close the letter, and on the Edit Attachment box, modify the Attachment name to letter-signed and press Save.

You will now see both letters in the Attachment window. Press OK.



The letter is now ready for the Analyst to export for their mail-out

24. EXPORTING YOUR RELEASE PACKAGE

Once a file is signed off by a Team Leader or an Assistant Director, the Analyst prepares the release package for the client. Depending on the size of the file, it will either be exported on CD or as hardcopy. Release packages are not typically sent to a client via email due to security concerns. Only True Access request replies may be sent to a client via email as the document being released has no security classification attached to it.

Note: All ATIP files have a 2 year retention period placed on them starting from the last administrative action placed on the file. Records are purged from the system once the 2 year time period is complete.

To export the records from redactions, go to the request drop down menu in Redaction, and select **Export / Print**.

EXPORT/PRINT

An Export/Print box will pop up. For all files, with the exception of ACs and PCs, fill in the following:

- **Type**: PDF Format
- **From**: Request
- **Save Location**: use the default or create your own on your H: drive (do not save onto your desktop)
- **Preset Option**: Release Package
- **Show Redactions as**: White
- **Pagination**: Off

Leave **Preview** checked off and then press **Export**.

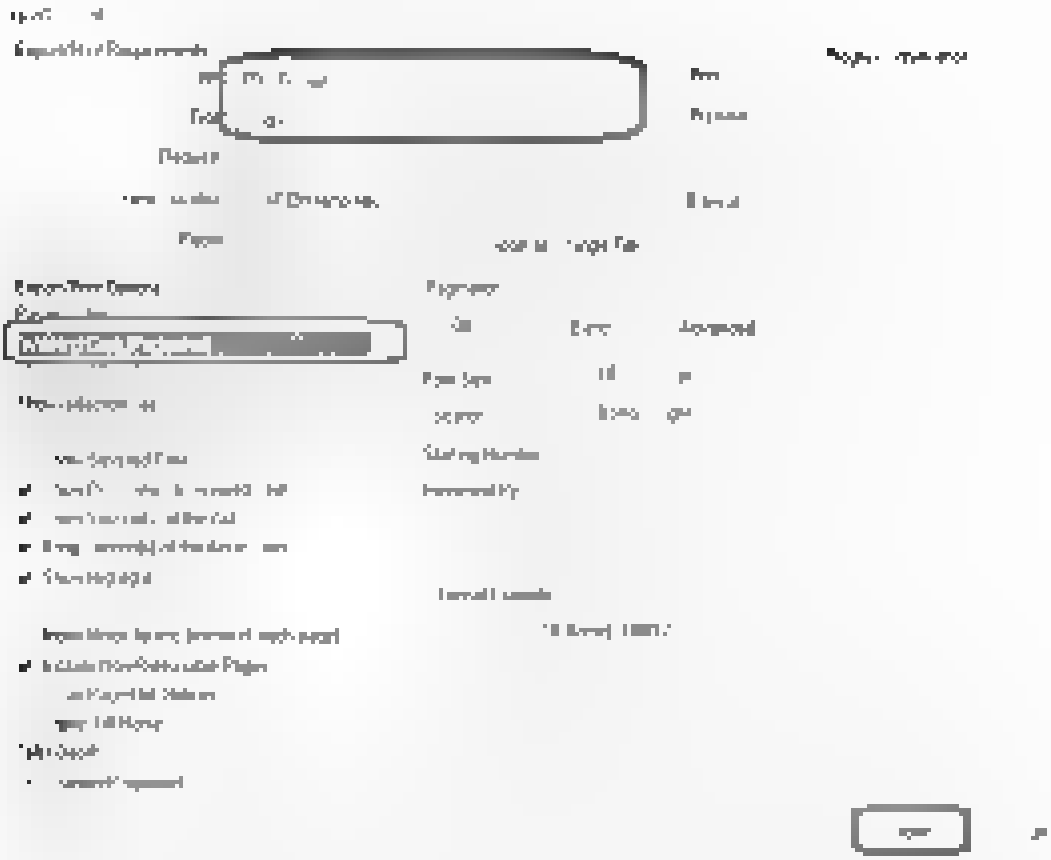
Your Release Package will pop up on your screen. You can press Exit now on your Export / Print box to close.

Note: Nil indicates that there is nothing to export – make sure that your records in Redaction are paginated.

For ATI or PA files, you will need to fill in the following:

- **Type:** PDF Format
- **From:** Request
- **Save Location:** use the default or create your own on your H: drive (do not save onto your desktop)
- **Preset Option:** Working Copy (Paginated)
- **Show Redactions as:** use default, grey
- **Pagination:** use default, basic

Leave **Preview** checked off and then press **Export.**



Quality Control

The PDF that this export produces is your Release Package. Place the Release Package on one screen and have Redaction open on the other (or do a split screen if you are working off one screen).

First, confirm that the total page count for your PDF matches the expected Released Pages in APCM. On occasion, the export will skip pages and you will have some pages missing. Next, scan through every Partial page and its corresponding page in the Release Package to verify that all severances have been applied.

Once you are done reviewing your release package, go to **Add Action, Mi- Closing** and select **Quality Control.**

Please close this action by entering the Date Completed as today once complete. You will also need to bring "Officer" over to the right by selecting it and pressing > before you press Save.

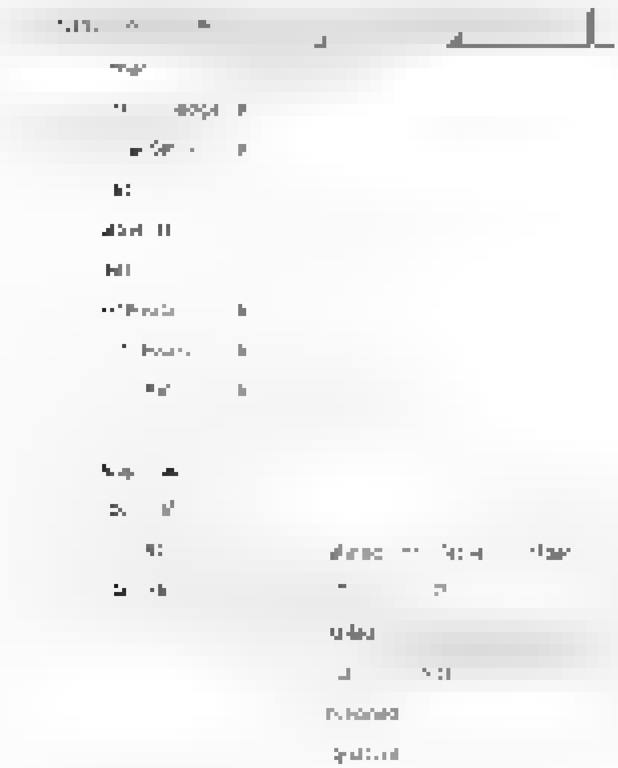
Once your release package is created and quality checked, your file is ready for mail-out. Refer to the next chapter for more information.

25. MAIL-OUT

The first step to prepare your package for mail-out is to add your **Mailed Out** action in APCM for the Operations Team.

Mailed Out

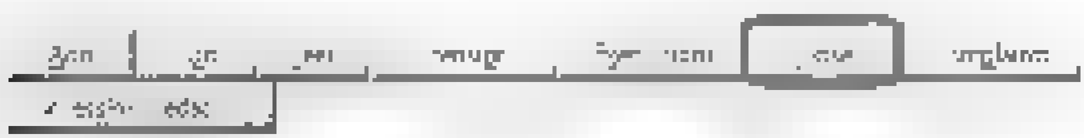
To add this action, go to Add Action, then M - Closing and select Mailed out.



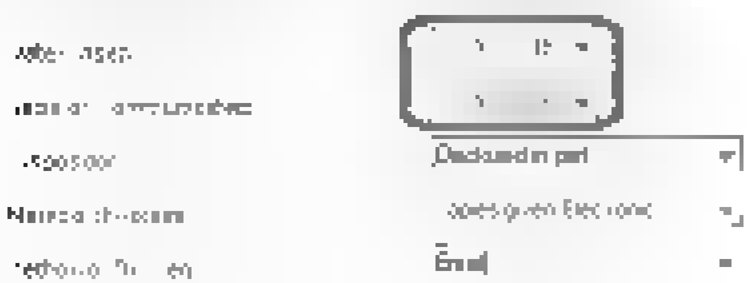
Once the Add Action box opens, type in *Operations* in the **Name field**, and press **Search**. If you are emailing the response, click on **Officer**. Next, press > to bring it to the right and type in "sent for mail-out" or "sent by email", today's date and your initials in the **Comment field**. Be sure to leave the **Date Completed** empty, unless you are emailing, in which case you may enter the date completed as today. Otherwise, the Operations team will enter **Date Completed** once they do the mail-out.

__Note:__ If there are special instructions in regard to mail out, you may put them in the Comment field.

If you have sent the response via email, you will close the file on your own. To do this, press the Close button in APCM.



A **Close Request** box will pop up. First, ensure that your *Disposition*, *Method of Access* and *Method of Delivery* are all properly entered. Next, enter today's date in **Date Closed** and **Date Communicated**, and press **Finish**. This will close the file.



Deleted from Retrieval Folder

Next, you will need to delete the folder/records from Acadia that were retrieved for this request, and close the **Deleted from Retrieval Folder** action line in APCM. To do this, fill in the **Date Completed** pertaining to the action in APCM as today, and press **Save**.

Lastly, do the following checks before you send for mail-out:

Records

- Check that all documents received are in Redaction (initial correspondence, payment, supporting docs).
- Records above Protected B must not be scanned into Redaction (use the standalone for docs up to Secret).

APCM Screen

- Ensure all actions are closed before the file is sent to the admin team (with appropriate dates), with the exception of the mail-out action.
- Verify if any Mandatory Actions (Delays and Complexity) have been added if applicable.
- Verify the number of pages reviewed and released under PROCESSED (this can be found by pressing the CLOSE button in APCM).

Exemptions Screen

- Ensure that any exemptions or exclusions applied to the records but not applied in Redaction have been added manually (this applies for records processed outside Redaction, i.e. SECRET). To manually apply exemptions/exclusions, press the Exemption button in APCM. Once the window opens, you can select the sections of the Act that you have used manually and press the > button to bring it to the right. Press **Save**.

Closing Screen

- Ensure that you have added your Disposition, Method of Access and Method of Delivery to your Closing Screen. See Closing Screen for more information.

Once all of your checks are done, create a folder specific to your request (if you haven't already) on your H: drive. Use one of the following naming conventions in naming our folder:

- BULK QA – FILE NUMBER – INITIAL
- LATE – FILE NUMBER – INITIAL (if applicable)
- CONSULT – FILE NUMBER – INITIAL (if applicable)

The naming conventions help the Operations team identify priorities for mail-out.

Next, place the Release Package that you have already quality checked in your H: drive folder. Single click on the RESPONSE letter action line in APCM, and once selected, press the **Attachment** button.

Select the signed version of the response letter and then press **View**.

Go to the File tab and then **Save As** to save the response letter, name it as the *file number response letter*, into your H: drive folder (in the same folder with your Response Package). Please change the File type, to save the letter as a PDF if it is a word document. Press **Save**.

Once the letter is saved, you can close the word application and click OK in the Attachment Box

Now that you have your release package and response letter in a folder, you are ready to drag and drop (or cut and paste) the folder into the Mail-out folder, for the Operations team

If the file is due the same day (today), or is late, put in the DUE TODAY folder

Note: Consultations always go into the DUE TODAY folder

If it is not due today, it can go in the regular mailout folder on the G: drive

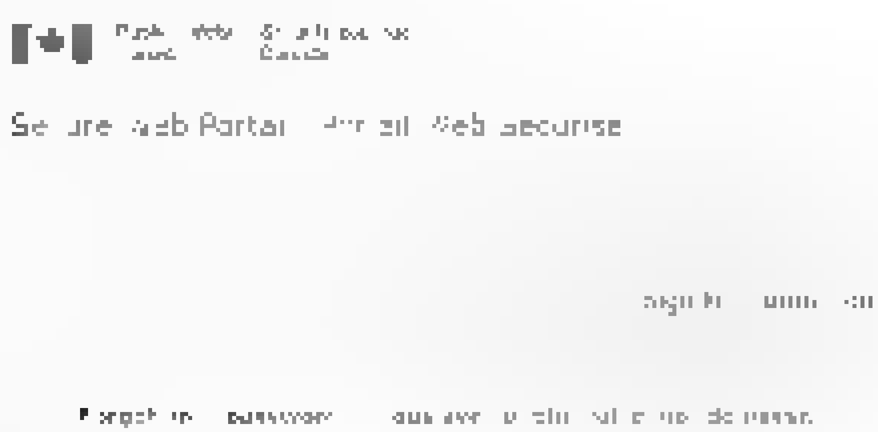
28. UPLOADING ONTO THE PUBLIC SAFETY PORTAL (True Access)

Below are the instructions on how to upload a release package to the Public Safety portal

These steps are only for True Access Requests, not for Access Consultations. Before you begin make sure that you saved your release package as "CBSA ATIP-A-2018-xxxxx (number of the request) Release Package". Then, go into APCM and copy the request text by highlighting it and pressing Ctrl+C to copy it

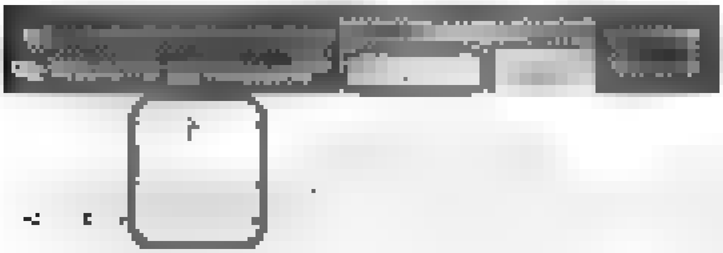
Next, click on this link

Enter your name and your password



Once you are logged in, under Requests, click on CBSA.

To add a document to the PS Portal, there are two processes. You can either go into the Documents tab (under Library Tools) and click on **Upload Document**, or scroll to the bottom of your screen and click on **+ Add Document**.



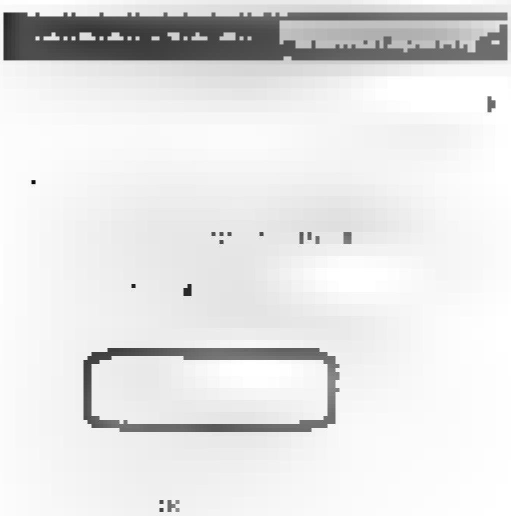
Next, an Upload Document window will pop open, click on Browse.

Find the directory and the file that you want to upload and double click on it. You can add any comments in the "Version Comments" section if this is another version of a file that you have already provided. When you are done, click **OK**.

Another pop-up window will appear. Enter the following:

- Request # box - type the request number
- Request Summary box - Press Ctrl-V to paste request text
- Key Topics box - type brief summary of topic
- Select the Calendar button for the Release Date and enter the release date
- Click on the Check-in button

The last step is to verify that your request has been added to the portal. To exit the portal, click on your name in the top right corner and select **Sign Out**.



27 RETRIEVING GCMS RECORDS

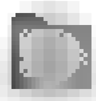
Your first step to retrieving GCMS records is to create a folder in Windows Explorer in the appropriate GCMS folder on the Shared Drive The new folder should be titled after the request number (ie. A-2018-XXXXX), with an "in prog." at the end to indicate that the GCMS retrieval is being worked on. This folder is where you will save all GCMS files that you retrieve. Once you are finished retrieving the GCMS files, remove the "in prog." from the folder name.

Next, open the newly created folder and click on **Date modified** twice (until the arrow above it points upwards). This will organize the incoming files by date and will help you keep track of them as you are downloading.

27.1 Logging into GCMS

To log into GCMS, follow the IRCC log-in screen located here

To log in, type in your < > and the password associated with the User ID. Once the IRCC page opens up, you will see 4 folders. Click on the GCMS folder



Next, click on the GCMS – Chrome icon

Your ID to access GCMS is and your password is the same as the one that you used for Citrix

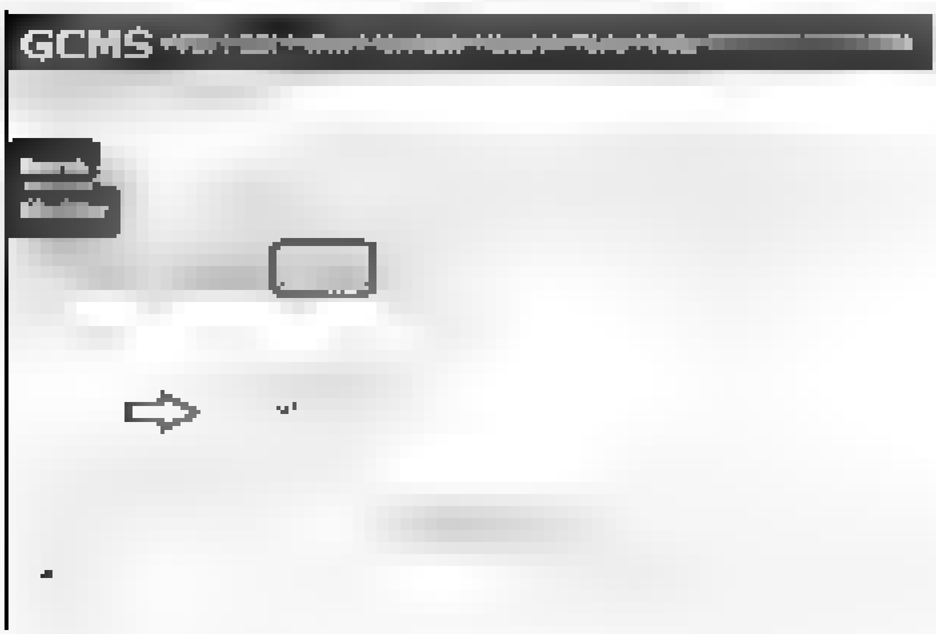
Once you are logged in, Click on three dots on the top right corner of the webpage

Next, click on **Settings**, scroll down and click on the **Advanced** option

Go down to the **Downloads** and turn on the "Ask where to save each file before downloading" option

27.2 Searching in GCMS

If the Client ID is provided, click on **Identifier** under the **Search** tab. In the 'Type' box select **UCI/FOSS ID** in the drop down menu, input the Client ID without any hyphens (e.g. 2345678) in the 'ID' box, and press **Search**.



A list will populate below in the **RDCC Integrated Search Hit List**; you will need to verify that the family name, given name and DOB match up with the request. If they do not, further clarification will be required. If they do, proceed to [GCMS Applications](#).

Note: It is the Analyst's task to provide the clerical staff with a Client ID number. Should there not be one included in the tasking email for GCMS, the clerical team should return to the analyst for clarification.

If a Client ID is not provided, go to the **Search** tab and then the **Integrated** tab. Fill out the family name, given name and DOB if you have it (enter it as YYYY/MM/DD), and press **Search**. If the search is slow, hit refresh one, two or three times, and it should finally produce a response.

The best suited matches will appear in the **IRCC Integrated Search Hit List**. If there are no perfect matches, further clarification will be required. If there is a perfect match, use the provided UCI to conduct a search as you would, had a Client ID been provided.

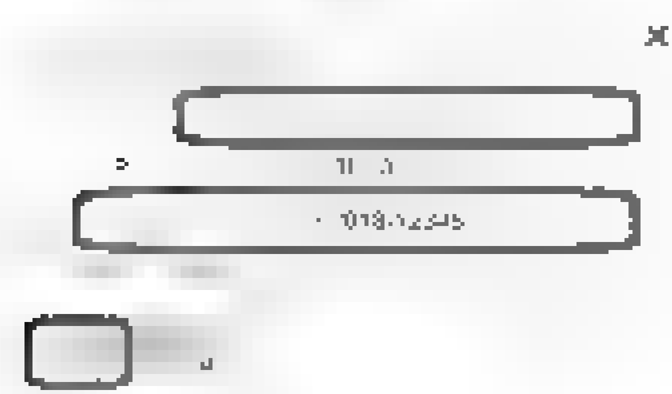
*Note: You have to confirm that the Client ID found using Integrated Search is truly that of the requested person. This can be achieved by confirming travel document numbers, current or former addresses, etc. in the applications or FOSS details.

27.3 GCMS Applications

Once you've found the correct individual, the list of applications associated to them will appear under **Person History**. The lines here are the applications that need to be retrieved and saved. It is possible a person will not have any applications associated to them. If that is the case, you may proceed to Retrieving CAIPS Records.

Applications are usually a letter followed by numbers. Click on each application number starting with the first one and then scroll to the top of your screen. Press the **Menu** button, scroll down in the menu, and then click on **Information Request**.

Next, an Information Request Box will pop up



Input the following:

Type: ATIP
Request Date – The 'Received Date' on the request
Request Identifier – ATIP File number
Report Language – The language the request was submitted in

Then press **Submit**

The relevant application will pop up. A disk icon should appear when you move your mouse over the bottom of the page. Press the disk to save the application into the Windows Explorer folder you previously created, and use the application number as the file name. If the information request reads CASE, add the word CASE before the application number. Once saved, close the application and press **Cancel** on the Information Request pop up to close. Next proceed to GCMS eDocs

Government of Canada Gouvernement du Canada

GCMS Information Request, Application

Requested For: 4/2018 ... 45

Requested Date: ... 10 ... 16

APPLICATION:

Created Date: 2018/04/28 12:04:28

Created By: EAMEL

Updated Date: 2018/10/23 10:25:02

Updated By: M104542

Primary Office: Los Angeles

Secondary Office: OSC - Operations Support Centre

App #: W123456789

Note: PPT Passport applications are not CBSA's responsibility to extract. When receiving the error message below, move on to the next application.

27.4 GCMS eDocs

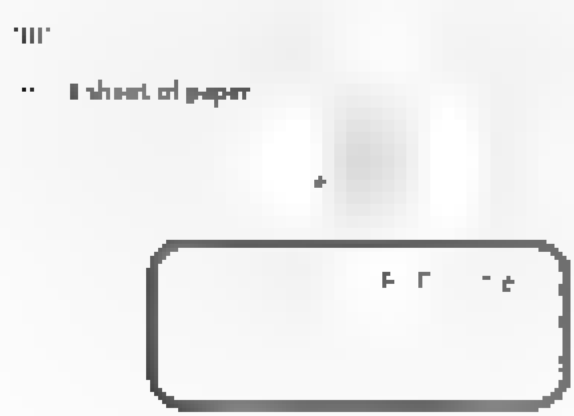
On the same application screen, click on the eDocs tab and the eDocs will populate below. If there are no eDocs or if there is no eDoc tab, proceed to GCMS Correspondence

If there are eDocs, open the first one by clicking on the eDoc number on the left. A save screen will pop up. Save the eDoc under the previously created Windows Explorer folder. Use the

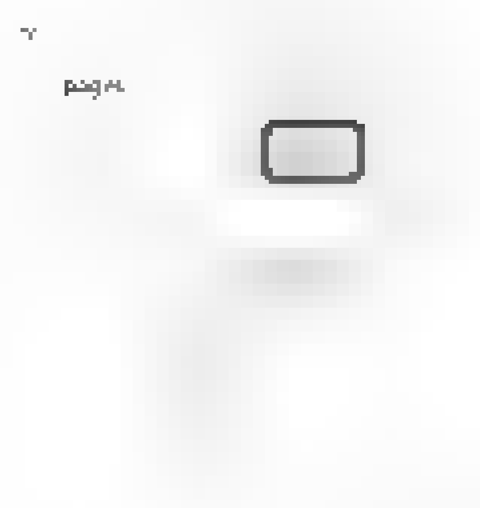
corresponding eDoc number from GCMS to name the file (Always copy the eDoc # and paste). Once you saved the eDoc in your folder, you can close the window pop up.

If the eDoc is an image, right click on the picture and click on "Save As". If you cannot right click on the picture (when the background is grey usually) expand the window and then right click on the white area, and select **Print**.

If the print **Destination** does not already indicate "Save as PDF", press the **Change** button and select **Save as PDF**. Again make sure you save to the correct folder.

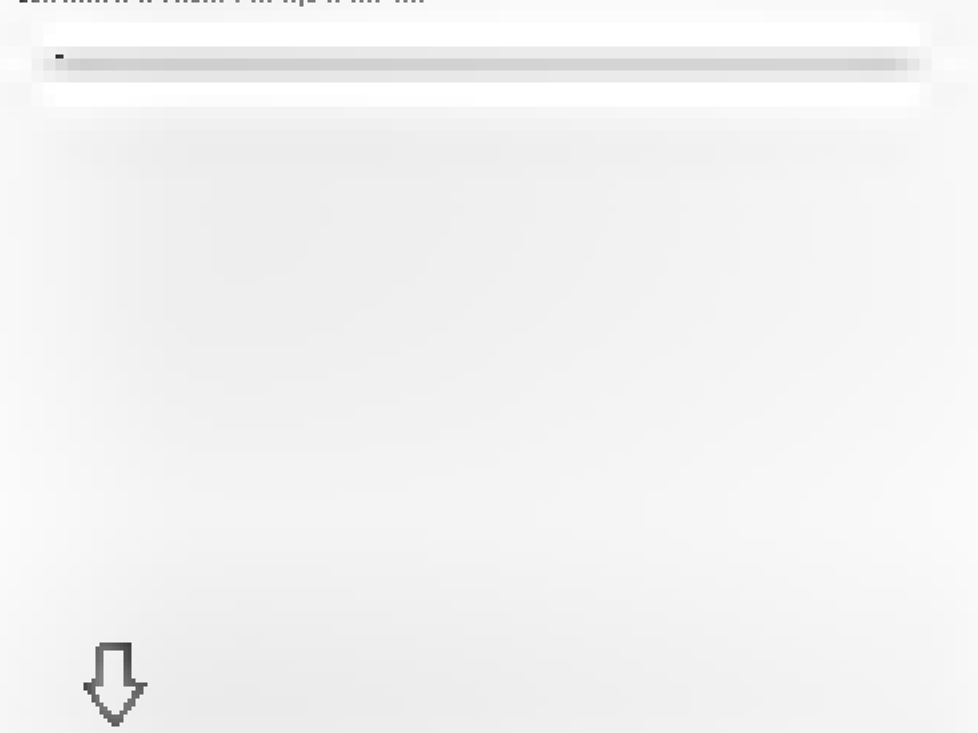


Next press **Save**, and this will create a PDF of the file.



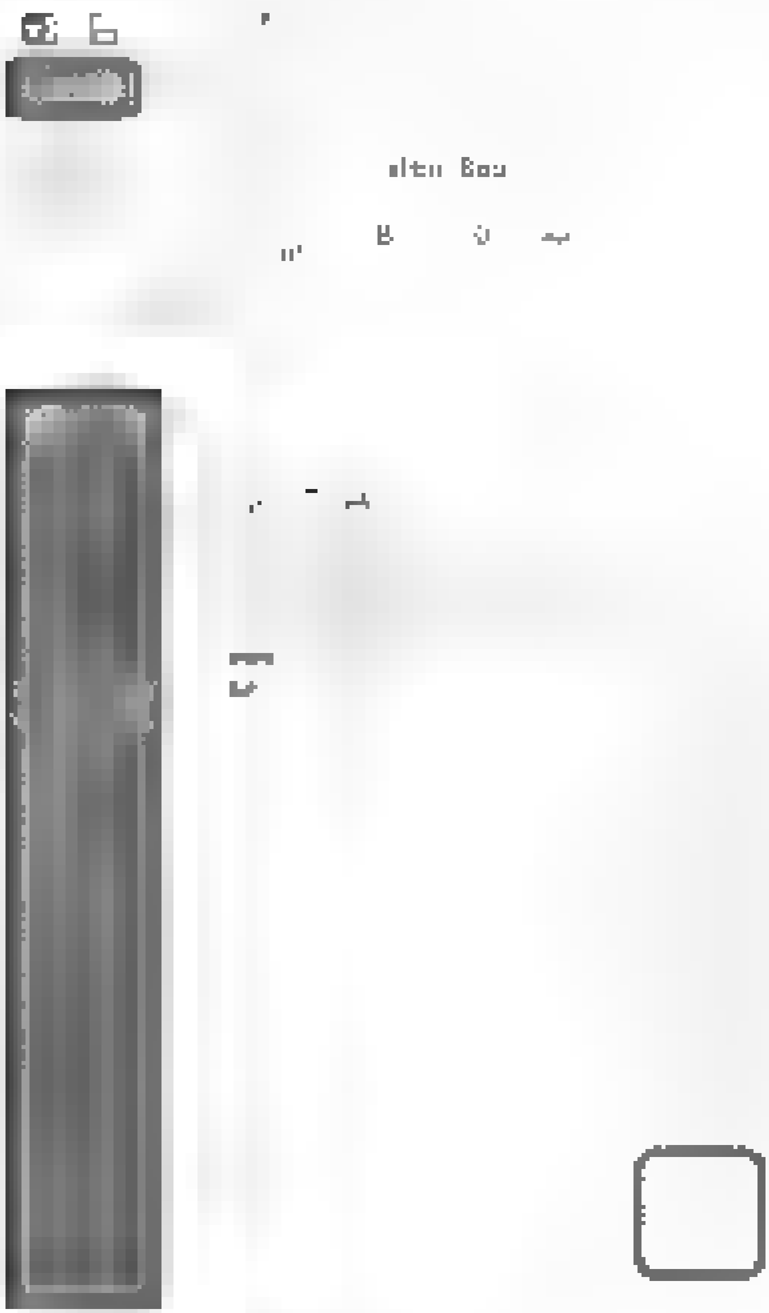
If the eDoc is a web page, right click anywhere on the page, and click **Print**. Again, if the **Destination** does not already indicate "Save as PDF", press the **Change** button and select **Save as PDF**. Next press **Save**, and it will create a PDF of the file. Make sure you save to the correct folder.

If the eDoc is a TIFF image file, a minimized window will open. Click on the file name on the bottom left corner to open the file.

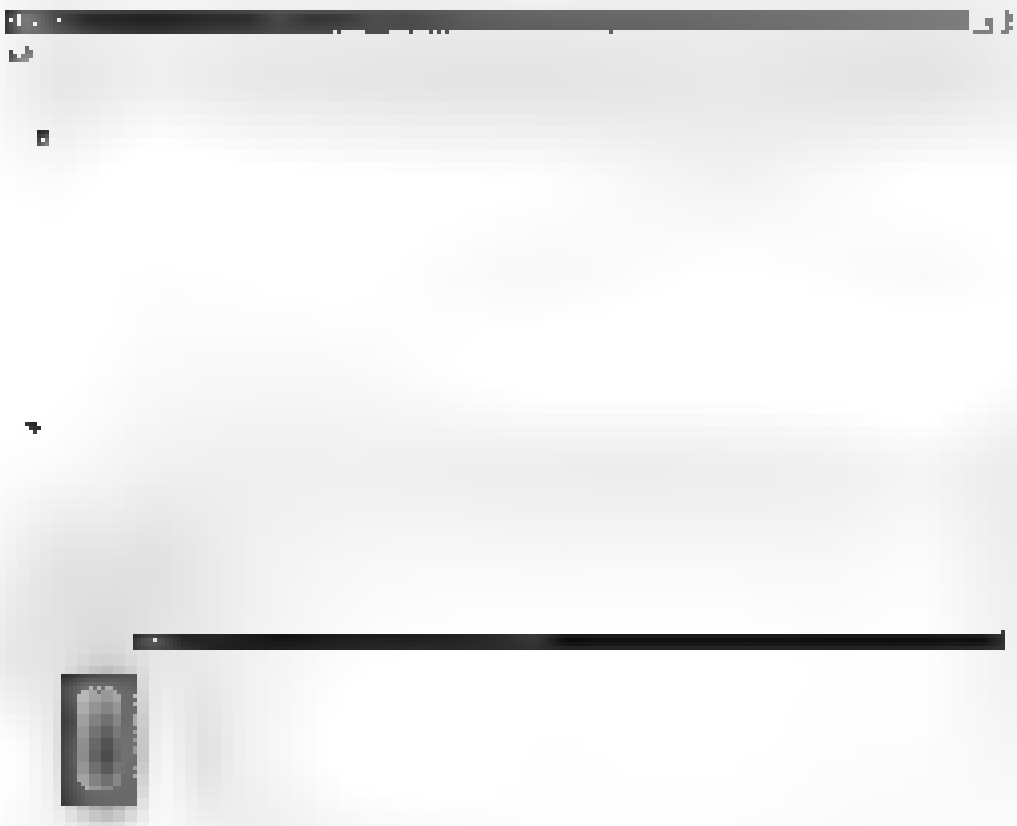


Once the file is opened, click on **File** in the top left corner and select **Make a Copy**. And make sure you save to the correct folder.

If the eCat is a Word file, click on the drop-down menu **File** in the top left corner, and select **Save As** and then **Browse**.

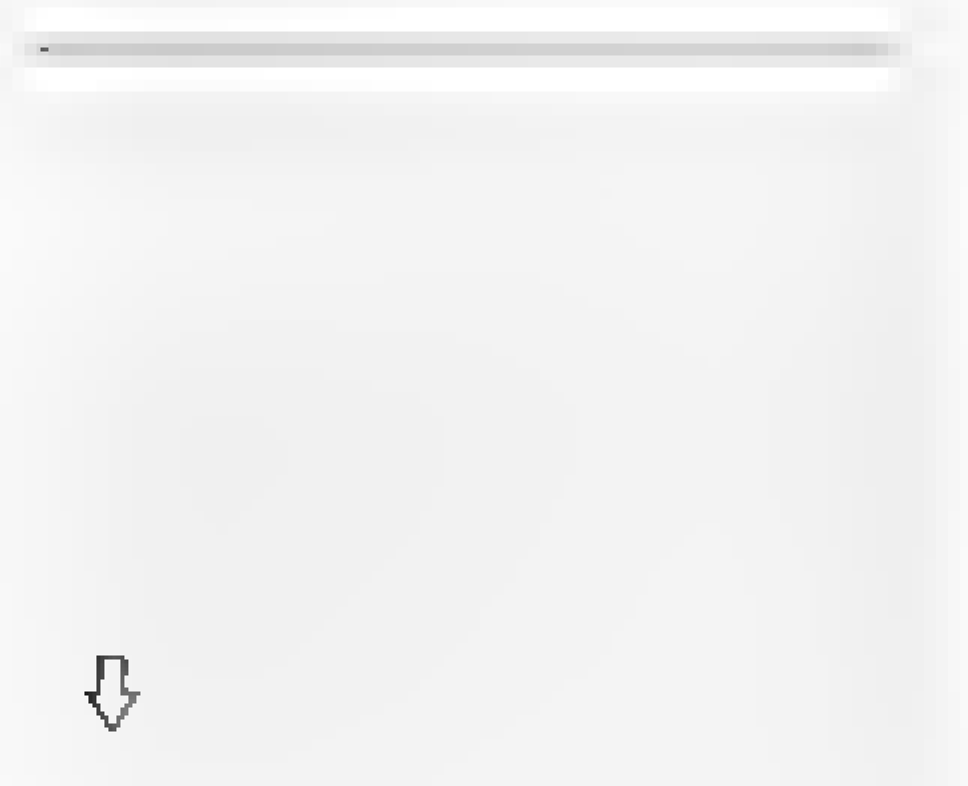


When the saving window appears, make sure you change the 'Save as Type' from Word to PDF. Then rename the file after the eDoc number. Make sure you save in the right folder.



If the eDoc is an XML file, right click anywhere on the page and click on 'Save As'. Again make sure you save to the correct folder.

If the error is an email, it will open in a box, minimized. Click on the message to open it in its entirety.



Once open, click on File and then **Save As** to save the email. Ensure you include any attachments in any of the emails you open. To save the attachments, click on each attachment individually, and once selected press the **Save As** icon at the top of the window. It is good practice to name the email by the eDoc number followed by "EMAIL" and then its attachments by the eDoc number followed by "ATTACHMENT1", "ATTACHMENT2" and so forth.

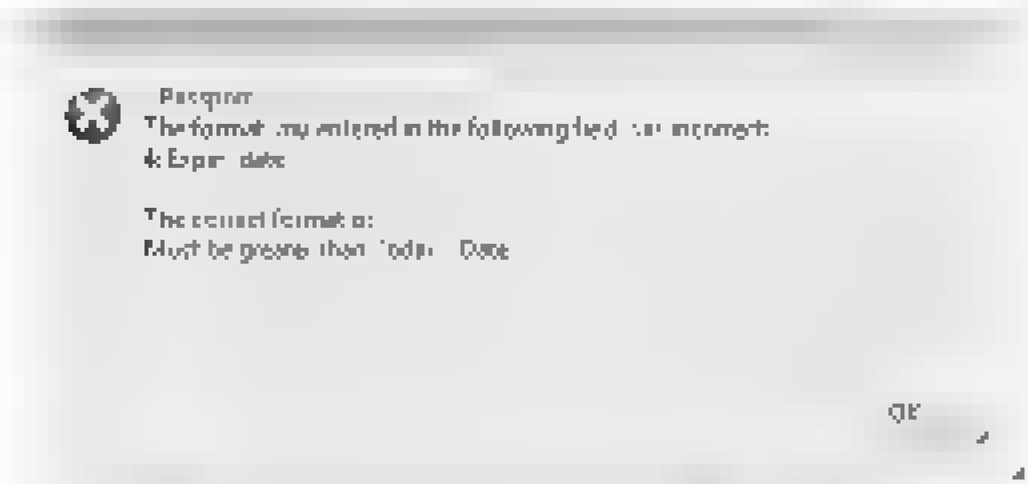
Save each of the eDocs in order from top to bottom on the list. Verify as well that there are no additional pages of eDocs. If you see 10+ on the right of the screen, there may be more eDocs. It is possible to have upwards of 30 eDocs for one application.

If 10+ does appear, you will then need to navigate to the next page by using the next button (at the bottom of your screen).

Once all of the eDocs are saved for that particular application, proceed to GCMS Correspondence.

TIP: Have your Windows Explorer folder open as you save the documents to ensure they are saved into the correct location.

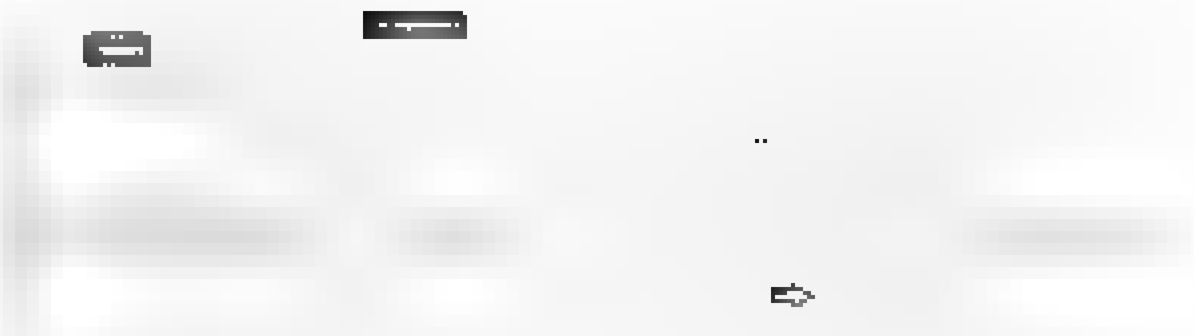
If you encounter a "Validation Error" when opening any eDoc, click OK until the eDoc opens.



Also if at any time the following Application Error pops up, ignore it and keep working on saving your opened eDoc. If you press OK or X, your eDoc will close before you can save it.

27.6 GCMS Correspondence

Once all of the eDocs are saved press the **Correspondence** tab in GCMS. It is possible that there is no correspondence tab, in which case, proceed to the next application and start these steps again. But if there are, start with the **Outgoing** correspondences.



In this window will verify against your Windows Explorer folder (as you saved all your eDocs by their eDoc #) that you haven't missed any eDocs pertaining to this client. With each correspondence line that you select you can see the relevant eDoc(s) in the **Correspondence Attachments** section. Click on each and every correspondence line item under **Outgoing** and if you find any eDoc numbers in the attachments section that you have missed, or any unnumbered eDocs, open them (by clicking on them) and save them into your Windows Explorer folder as well. Rename the files so that they correspond with the name on GCMS (copy and paste).

If you are prompted to do a File Download when discovering a new eDoc through Correspondence attachments, press **Download**.

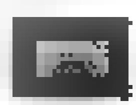
If the file is an Email (ex: Email 123456789-HDF6G7), it will open directly. Right click on the window and select **Print**. If the **Destination** does not already indicate "Save as PDF", press the **Change** button and change it to **Save as PDF**.

sheet of paper

Next press Save, and it will create a PDF of the file

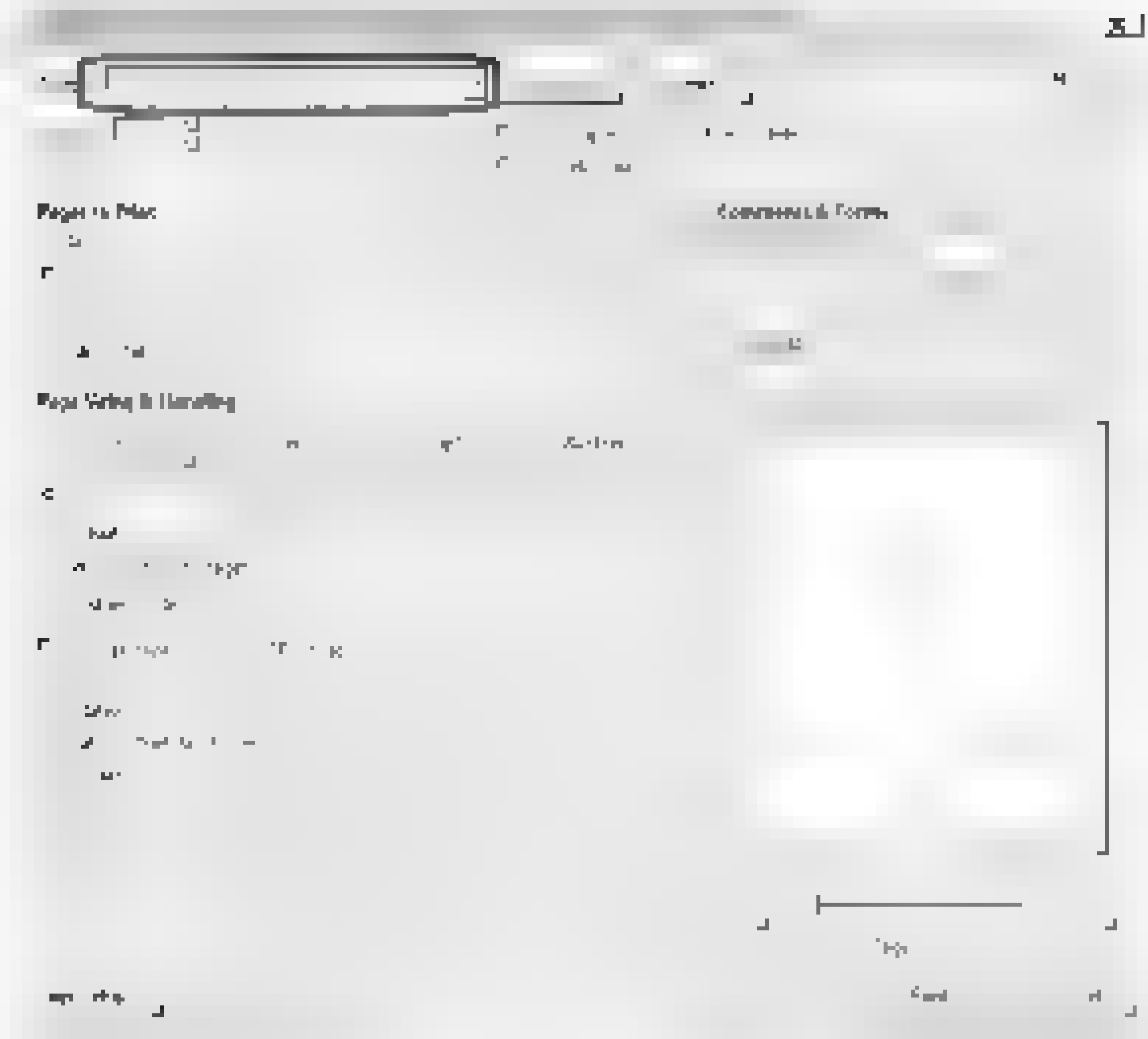
If the attachment is a PDF (ex. IMM5017, A12345, Auto Email 123456, etc.) click on the file name in the bottom left corner of the window to open the file

To save these, click on the Disk Icon in the top left corner



IMPORTANT NOTE: If the save icon is not in the top left corner but instead at the bottom of the page, do not save as you normally would by pressing the disk icon, otherwise, the saved document will be missing information. This occurs mainly for **DEPARTURE ORDERS and REPORTS UNDER 44(1)** (files in examinations (ex: N-123456789).

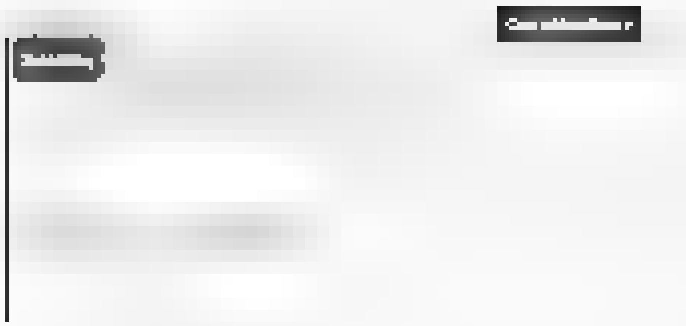
Instead, click on the **printer icon** instead of the Disc icon and select **Microsoft XPS Document Writer** as the printer and click **Print**. A Windows Explorer window will open. Save the file in the proper Windows Explorer folder.



If at any time the attachment is called Word [illegible] (the number will vary) simply ignore the attachment and move on to the next one. These are templates that are not filled out with information.

Again make sure you look for [illegible] on the right to ensure there are no additional pages to navigate through.

Once you are done verifying the Outgoing Correspondence, select **Incoming Correspondence** and do the same things. For Incoming, your **Attachments** section is across the bottom of the screen, not on the bottom right.



Again make sure you look for 1/1 on the right to ensure there are no additional pages to navigate through.

Again, if at any time the following Application Error pops up, ignore it and keep working on saving your opened eDoc. If you press **OK** or X, your eDoc will close before you can save it.

When all correspondence is saved and verified, repeat the same process with the following applications. To proceed to the next application head back to the **Search** tab and then back to **Person History**. Once every Application, its eDocs and correspondence is saved, proceed to CAIPS Records.

27.6 CAIPS Records

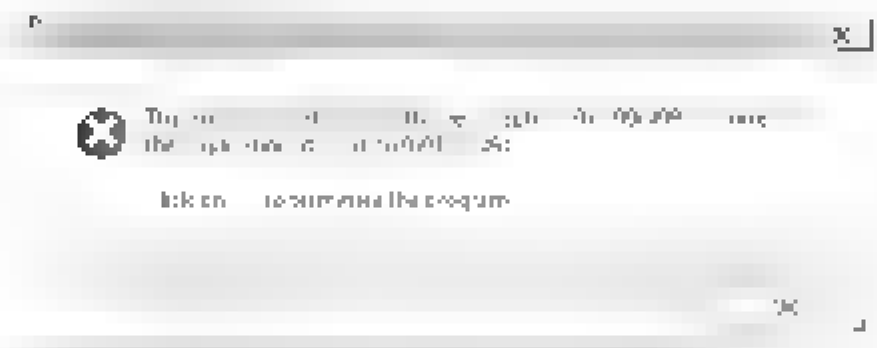
Now that you have saved all the relevant GCMS applications and their eDocs, the last step is to check to see if there are any CAIPS records to retrieve. To check for these records, return to the **Search** tab, and look to see if the **Get FOSS Details** button is blue. If it is grayed out, there are no FOSS records (which is where you will find the CAIPS records) and you can proceed to Printing your GCMS Records into Redaction. If it is blue, press the **Get FOSS Details** button to proceed.

Once you press the button, scroll down to the FOSS section on your screen in GCMS. In this section you will want to click on each and every line to see if, when the line is selected, the **Get CAIPS Details** button turns blue. If it is greyed out, there are no CAIPS records.

However, if you find a line that changes the button to blue, there are CAIPS records to be found within it. Press the **Get CAIPS Details** and the CAIPS record related to the line item will pop up. Highlight your mouse on the bottom of the image so that the disc icon appears and save the CAIPS records along with your Applications and eDocs in Windows Explorer folder you had created. Name it as: CAIPS_[doc#]_[line#] as a pdf.

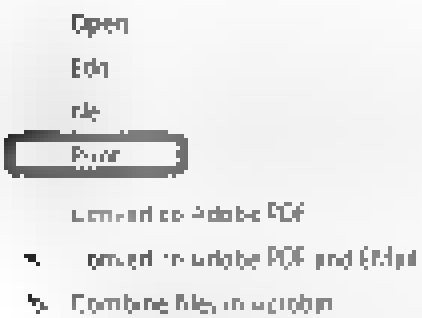
Once all CAIPS are saved, proceed to Printing your GCMS Records into Redaction.

And once again, if at any time the following Application Error pops up, ignore it and keep working on saving your opened eDoc. If you press OK or X, your eDoc will close before you can save it.

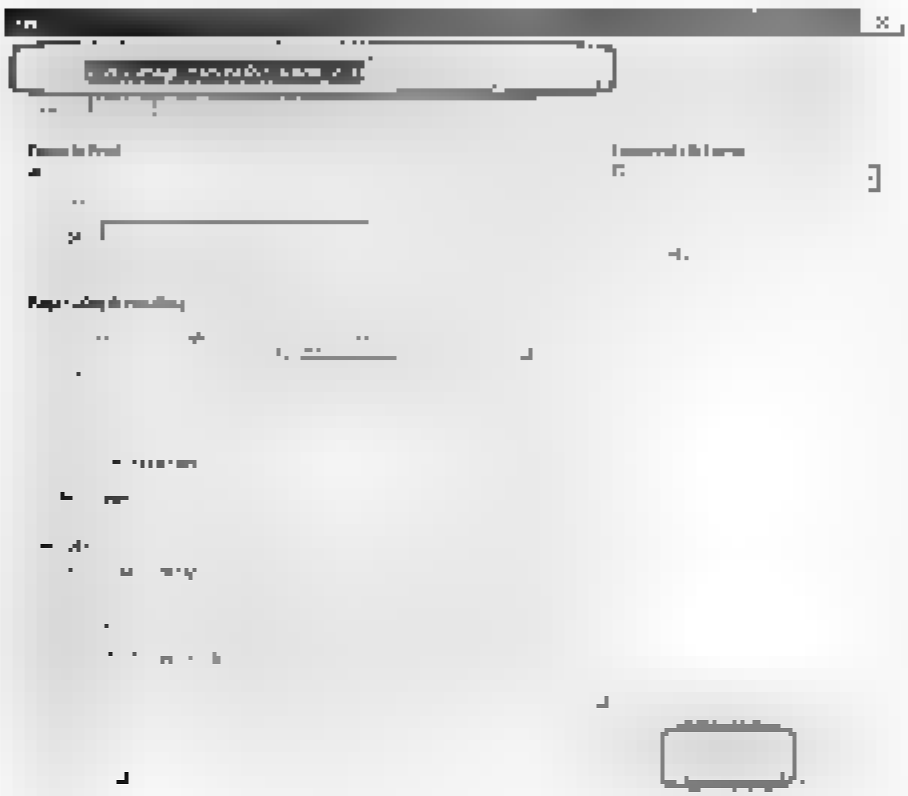


27.7 Printing your Records into Redaction

Your next step is to go back into your Windows Explorer folder holding your GCMS, FOSS, eDocs and CAIPs records and you will need to right click on each file separately, and select **Print**.



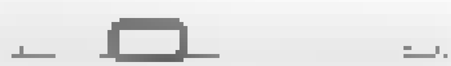
When the Print window pops up, change your **Printer** to **Print 2 Image** and then press **Print**.



Next the Print to AccessPro Redaction box will pop up. Ensure the correct Request Number has populated, and select the relevant stacks. If the GCMS, EDOCS and RCD stacks are not created in Redaction, you will need to create them. For GCMS applications and CAIPS files, select **GCMS** and **RCD** (to select two stacks simultaneously press the **Ctrl** key before you select your second stack). For any eDocs, select **EDOCS** and **RCD**. Once you have selected the relevant stacks, press **OK**. Repeat this step for all files in your Windows folder.

The final step is to go back into APCM, double click on the **SYSTEM NOTES** line pertaining to GCMS and indicate the number of pages that were inputted into Redaction in the comments field and your initials (ie. Printed 28 pages into redaction - SS). Copy the comment as you will need it in the next step. Input Date Completed as today's date and press **Save**.

Lastly, click on **Email** in APCM.



And a Select Template box will open. Click the **GCMS Completed** template and press **Select**.

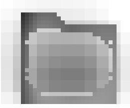
An Outlook window will open. Paste the comment that you previously copied in the email and then press Send

You can now proceed to your next GCMS request

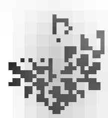
28. RETRIEVING FOSS RECORDS

To retrieve FOSS records, the first step is to follow the IRCC log in link below.

To log in, type in your [illegible] and the password associated with the user ID. Once the IRCC page opens up, you will see 4 folders. Click on the **Data Warehouse** folder.



Select Cognos BI.

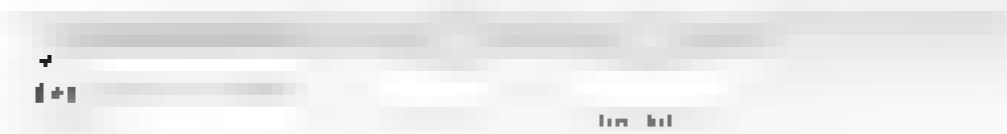


This will open up a new window – IBM Cognos Software

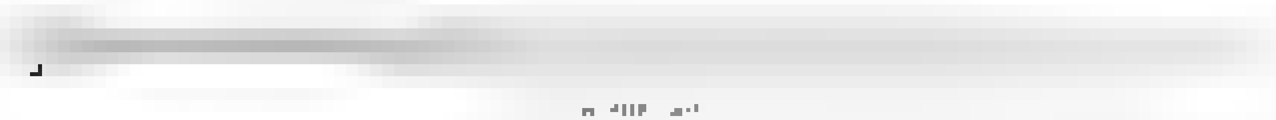
Next, in the address bar above, erase the default web address and paste the following web address:

Once the new address is pasted in, press **Enter** and a new window will open.

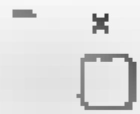
Choose your language of preference – **English** or **French**.



Enter your User ID and **Password** (these are the same as the ones you used in the first login screen). This will bring you to the FOSS ATIP search screen.



On the top right of the screen, click on the tool icon to open the 'Print' and then the 'Page Setup' box.

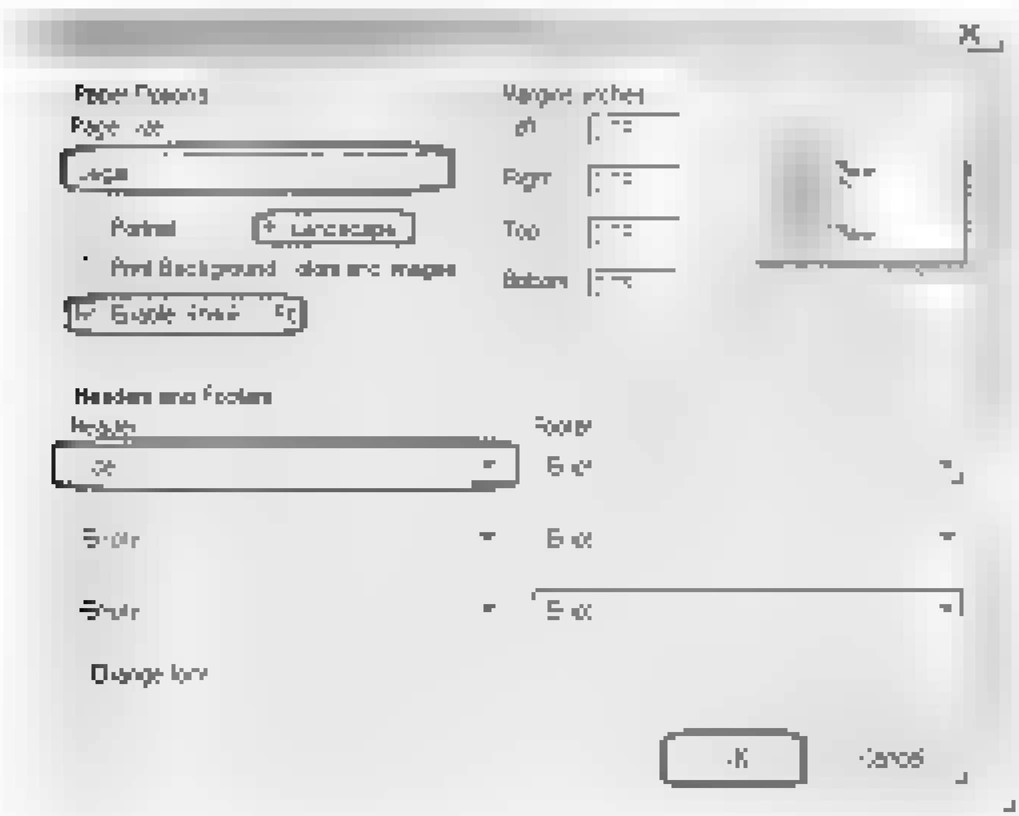


Select the following:

- **Paper Size** = Legal
- **Orientation** = Landscape
- Click on **Enable Shrink-to-Fit**
- In Headers and Footers the first Header should be **"Title"** and the rest **"Empty"**

Then click **OK**.

<u>Note:</u> This page setup has to be redone every time you log on. It cannot be saved.

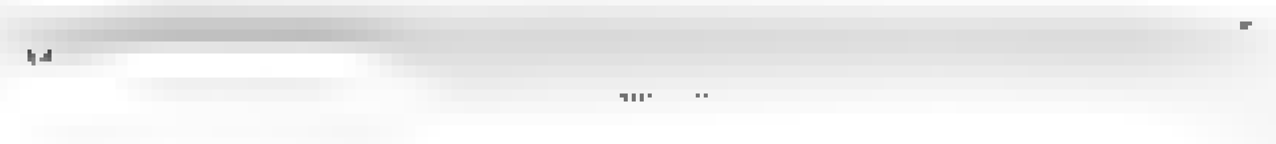


Go to the Generic ATIP email account, and to the "FOSS" Inbox folder and select the oldest email tasking. Drag the email under your name and open it.

Search for the file number in APCM, and open the file in both APCM and Redaction.

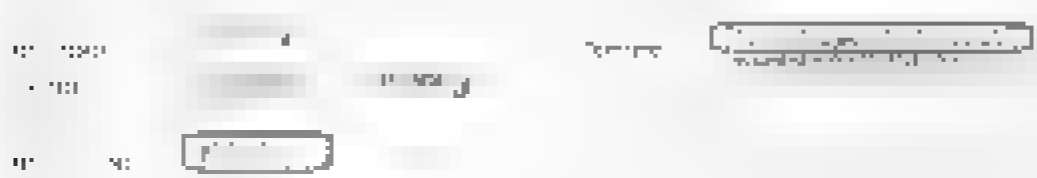
Ensure that the appropriate stack has been created for FOSS. If it hasn't been, you can create it. The section Printing to Redaction, Stacking and Indexing explains how print to do this, and Annex C: Stacking and Indexing shows the various naming conventions used.

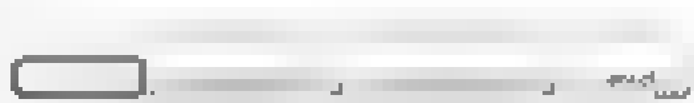
Go back to your FOSS Search screen and input the Client/FOSS ID number, select English or French depending on the language of the request, and press **Search**.



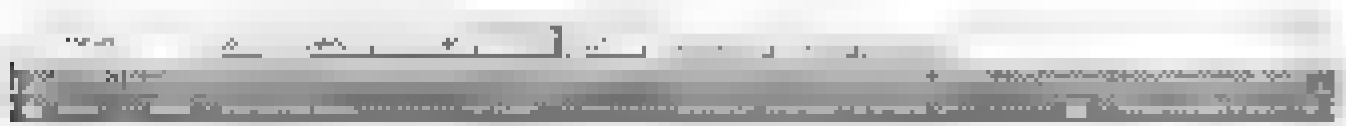
Check to see if the name matches (either in the title of the FOSS page or in the aliases) and then "Print-2-Image", choosing the correct file number and the FOSS Stack. Next, press **Refresh** and name the document "FOSS notes".

In APCM, double click on the **FOSS** retrieval action line and close the action by completing the **Date Completed** as today's date. In the Comments section, write: "Printed (# of pages) FOSS notes (initials)". Highlight your text & copy (by pressing Ctrl + C) and then press **Save**.

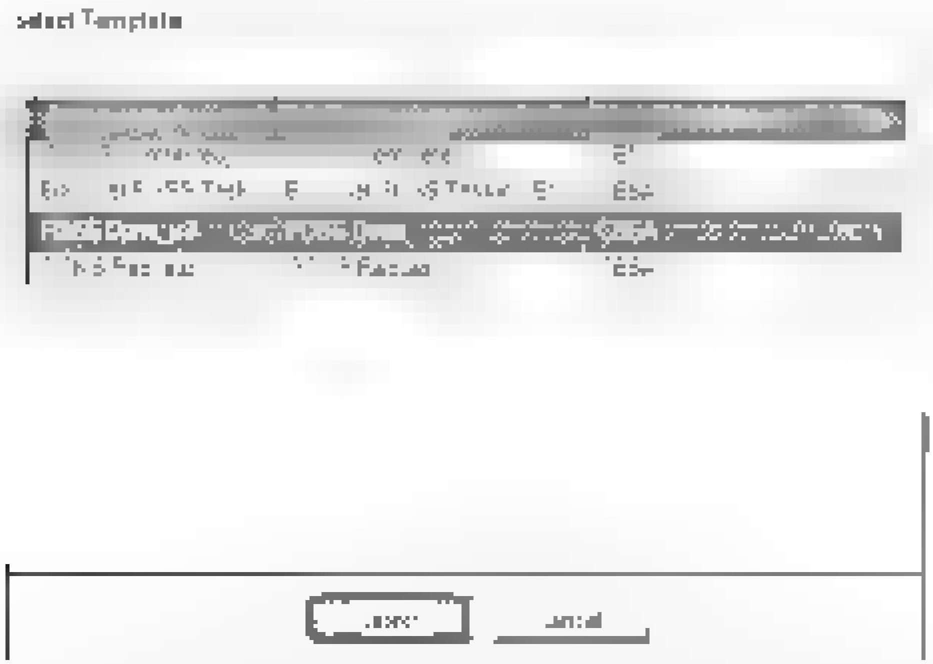




Select again (click once) the **FOSS** retrieval action line and press the **Email** button.



Once the Select Template box pops up, choose **FOSS Done v3** and press **Select**.



At the top of the email, paste (Ctrl+V) the text that you copied above indicating the number of FOSS pages, and send the email to the Analyst. Once the email is sent, move the original FOSS Retrieval email into your done folder.

29. AUDIO / VIDEO FILES

Occasionally the ATIP Division receives requests for [illegible] that include audio / video files, and since we do not yet have the means to vet these types of records internally, we work with [illegible] Science & Engineering – Border Technology (BTD), in order to respond to these types of requests.

Types of audio / video records reviewed may include:

Audio / Video: Interviews between a client and a CBSA Officer

- Often on an immigration file, there is also a transcript included of these interviews. If this is the case it may be possible to negotiate with the client to omit audio / video from their request, explaining that they will be receiving the same information in a transcript format and by omitting audio / video it can possibly expedite their request more quickly.
- When listening to this type of audio, please ensure you listen for background noise. In some types of these interviews, multiple people were interviewed at the same time in [illegible] and background voices of other interviewees may be possible to hear.

Video: Footage from a border crossing containing images of the client

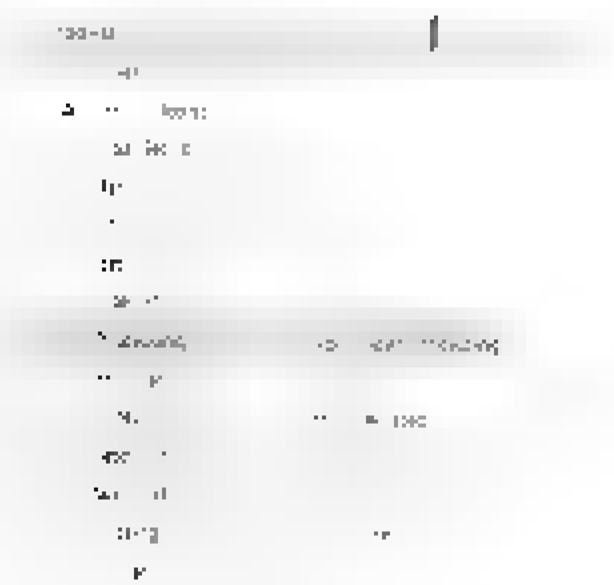
- For these types of requests, you will likely require a photo of the client (if one is not already provided) in order to identify them in the video. Also discuss with the client exactly what element they are seeking (video of a specific moment at the crossing?) and try to negotiate the scope of their request down to only the video they require to expedite their request. Most clients will be reasonable as they would like their information as soon as possible.

If the complexity of the vetting process is too great for any video, speak with your Team Leader or Assistant Director, as a decision can also be made on whether or not the client will be granted only viewing privileges at a local CBSA office, and they would have to attend the location to view the record and they will not receive a copy of the video.

The specifics of the Audio / Video vetting process will involve only one point of contact for each Division:

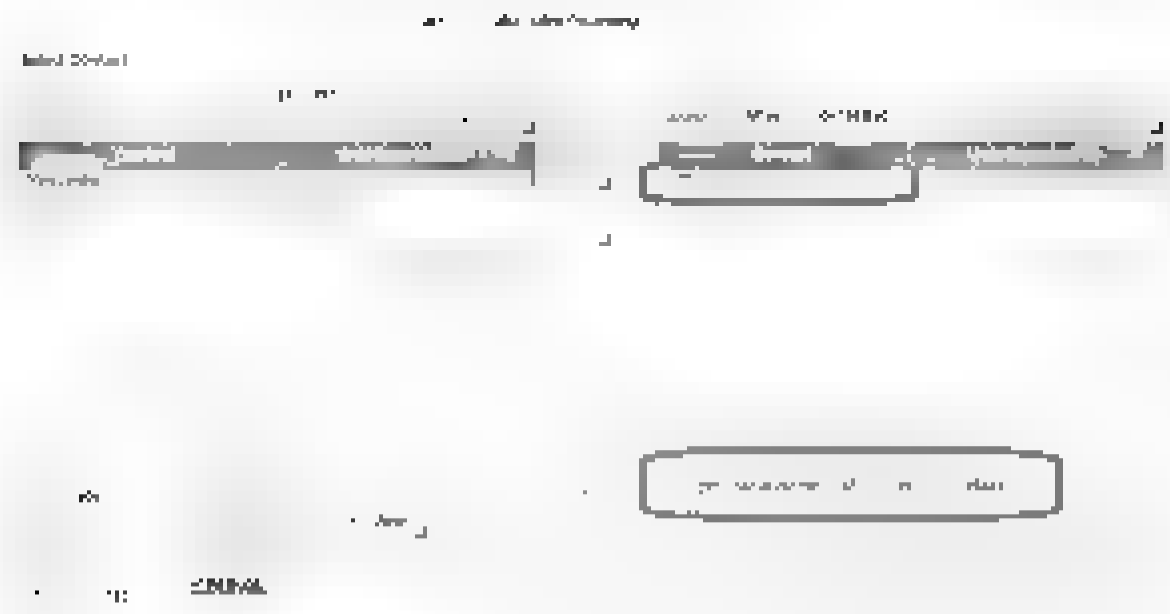
- ATIP Division: [illegible]
- [illegible] Division: [illegible]

If the action isn't already present on your file, to add the Audio/Video Processing action, go to Add Action > [illegible] **Processing** and then select **Audio/Video Processing**.



First and foremost, review the content of the audio / video file

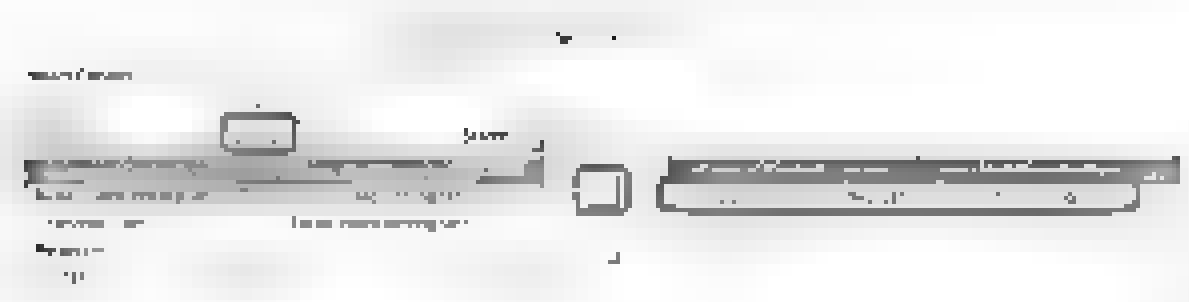
If the audio/video <u>does not</u> require editing, in your action box select Officer and press > to bring it to the right. You may record any notes relevant to your audio/video. In this example, you have reviewed the records and deemed them ok for release. You may close the action with today's date and press **Save**

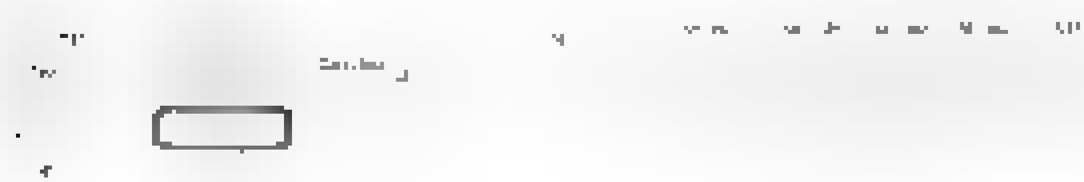


29.1 The Vetting Process of Audio/ Video

If you need to send a video to BTD, ensure that you are able to locate the client in the video. If it is not obvious which person on the video is the client, you will have to contact them to provide a suitable picture that is good enough quality to allow us to identify them. If you need a picture, add an AwaIncomplete action to the file, draft a letter explaining to the client that we require a picture to process the video files and place the file on hold. When all the information needed is received you can then proceed.

To start the vetting process, open your Audio/Video Processing action in APCM, and type in "audio" in the Unit/Organization field, and press **Search**. Once found, select **ATIP Liaison, Audio Video Lab** and press > to bring it to the right. Note where your records originated, their duration, your initials and date as in the example below. Leave Date Completed blank as the action is still ongoing. You may use this action box to record any happenings of your audio/video records as they occur. Press **Save**.

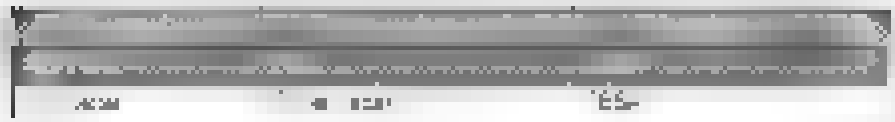




Now in APCM, select the Audio/Video Processing action line you just created. And press the **Letter** button

A Select Template box will pop up. Choose A-V Form and press Select

Select Template



Select Cancel

Complete the Audio/Video Form to the best of your ability; there are examples in the form to guide you. The purpose of this document is to outline the type of recording that needs to be vetted (audio or video) as well as what needs to be vetted from the file. You will have to review the material being sent and provide the start and end times for the segments that need to be enhanced. Please be as precise with the time as possible to ensure that the lab (BTD) enhance the proper information. Also, where required, please provide a description of the information that is to be vetted (e.g. desired outcome).

For Officer Name, type "Marco Vallee marco.vallee@cbsa-asfc.gc.ca for (your name)". Marco is our liaison between our division and the BTD. Print a copy of this form, and then press the X in the top right of your screen to close.

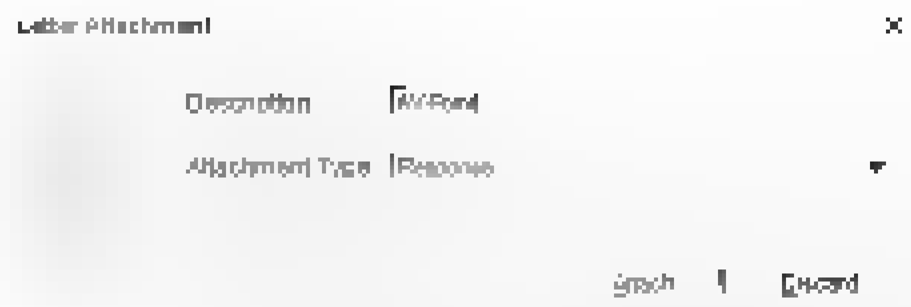
Microsoft Word ✕

Want to save your changes to
[illegible].doc

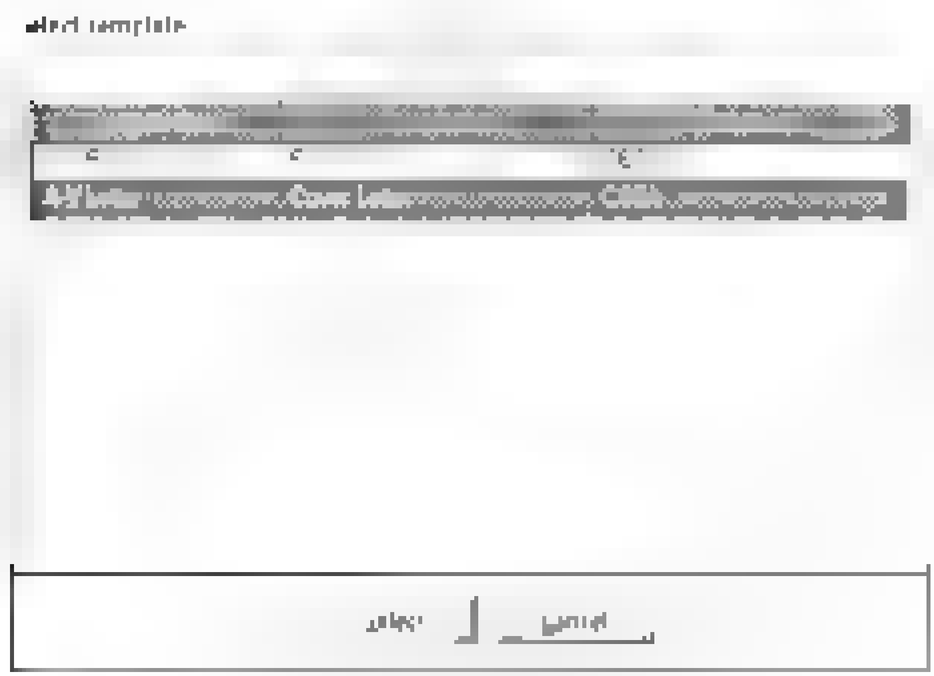
If you click "Don't Save", a recent copy of this file will be temporarily available.

Save Don't Save Cancel

A box will now pop up prompting you to save. Press **Save**. Next, a Select Attachment box will appear. Type in A/V Form in the Description field, and press **Attach**.



Now in APCM, select the Audio/Video Processing action line again. And press the **Letter** button once more. This time, when the Select Template box pops up, choose A-V Letter and press **Select**.



Once the letter appears, edit it to reflect whether or not it was an Audio or Video file, print a copy of this letter and sign it. Then press the X in the top right of your screen to close.

Microsoft Word

Want to save your changes to
APCM2030[illegible].doc?

If you click "Don't Save", a recent copy of this file will be temporarily available.

Save | Don't Save | Cancel

A box will now pop up prompting you to save. Press Save. Next, a Letter Attachment box will appear, type in AV Letter in the Description field, and press Attach.

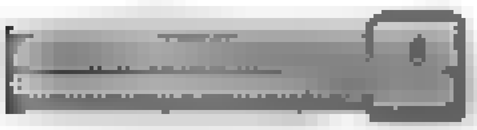
Letter Attachment

Description: AV Letter

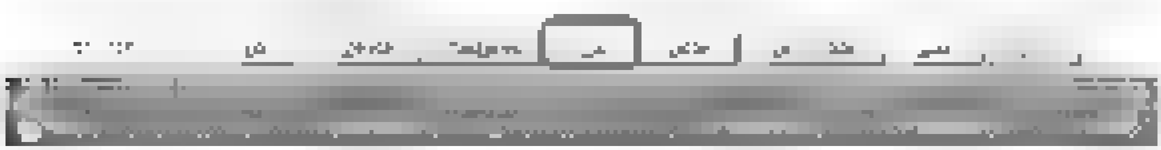
Attachment Type: Reasons

Attach | Discard

In APCM you will now see both attachments in the last column of your action line.



Select this line, once more and now press Email to send Marco an email to notify him of the vetting request and deliver the hardcopies of your signed letter and form, and a CD-ROM copy of your records to him. Important: Please ensure that the media you provide is the best available copy or the original copy available.



Marco will then assume the liaison role between the division and BIO. Once the vetting is complete, he will advise you.

30 COMPLAINTS

[illegible]

[illegible]

[illegible] in the official language requested by the individual.

30.1 Receiving Complaints

[illegible]

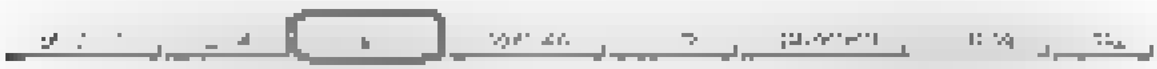
[illegible]

[illegible]

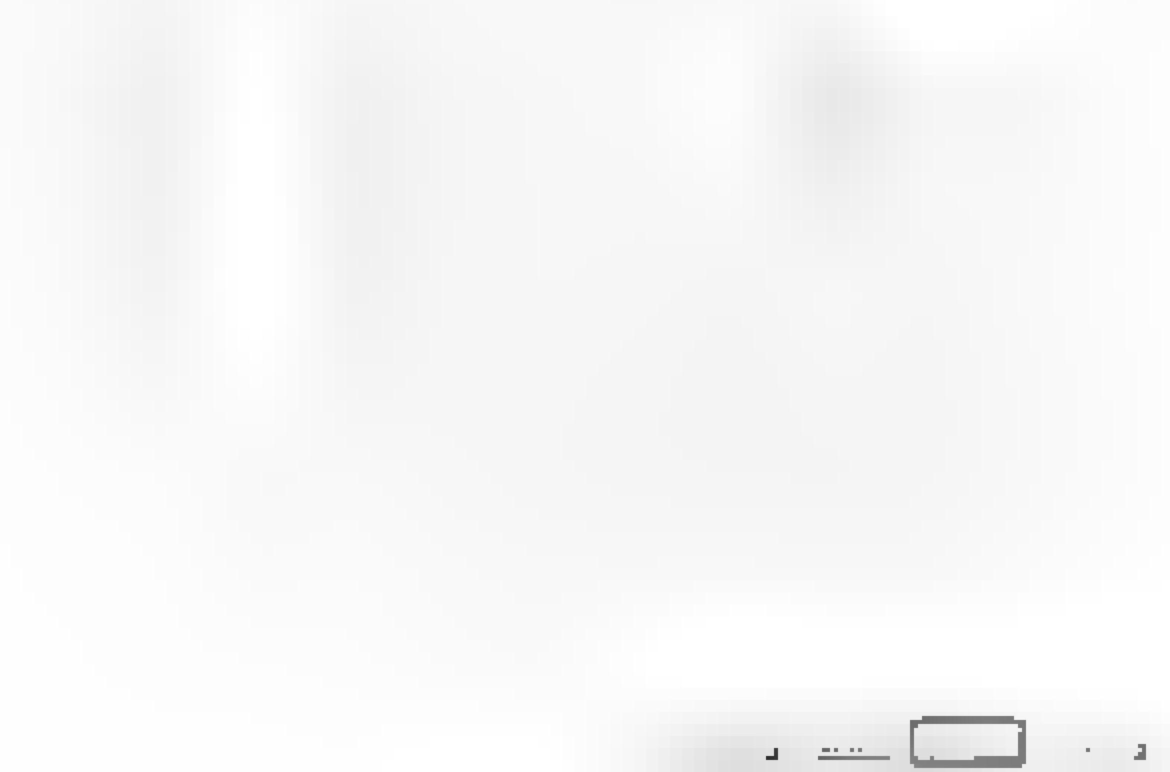
[illegible]

30.2 Logging a Complaint into APCM

To add a complaint into the complaint tab, press the **Complaints** button at the top of the screen in APCM.



In the Complaints box, press the **Add** button. Once the screen opens, complete the following: Date Complaint Received by the CBSA, Officer Assigned (Complaint Coordinator until such a time as an Analyst is assigned), Complaint Number, Date Received by Commissioner, Reason, Complaint Text. Once the fields are completed, press **Finish**.



Back on the Complaints screen, press **OK**.

30.3 Recording a Complaint Received Action in APCM

COMPLAINT received

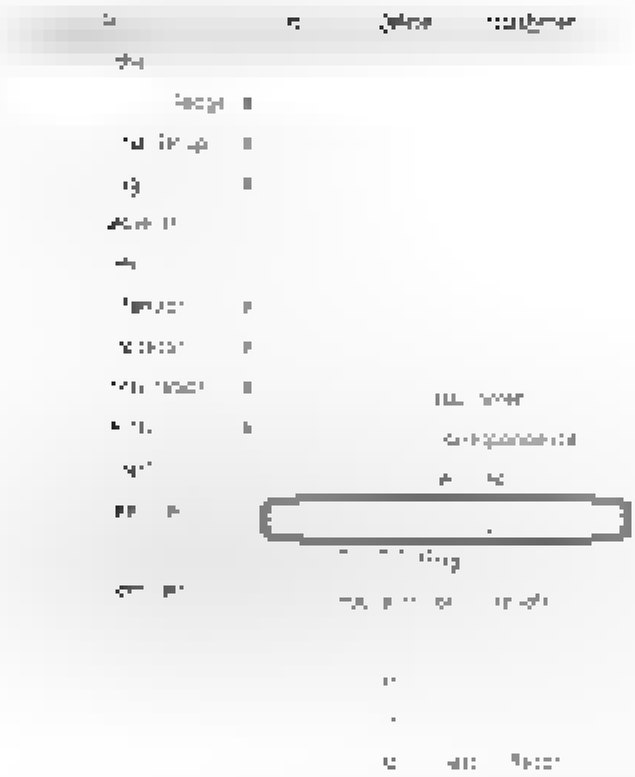
The Complaint Coordinator is responsible to add the **COMPLAINT received** action in APCM. This is done by pressing the **Add Action**, **O-Complaints**, and select **COMPLAINT received.**

Once the **COMPLAINT received** Action Screen opens, search for the Complaint Coordinator's last name in the name field. Once found, select it and press > to bring it to the right hand side. The Date Created corresponds to the date the complaint was received by the CBSA. For the Due Date, press **Calculate** and a due date will auto populate. In the Comments section, enter your initials. Once the information is inputted, press **Save**. This action is to remain open until the complaint has been resolved (formally grounded by the Commissioner's office.

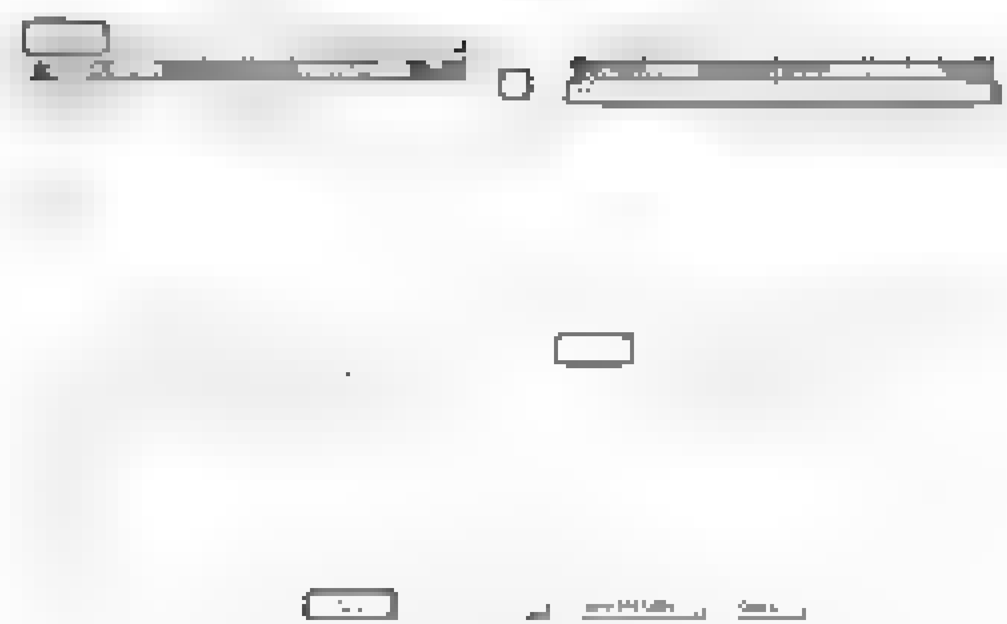
30.4 Recording the Investigator Package Action in APCM

Investigator Package

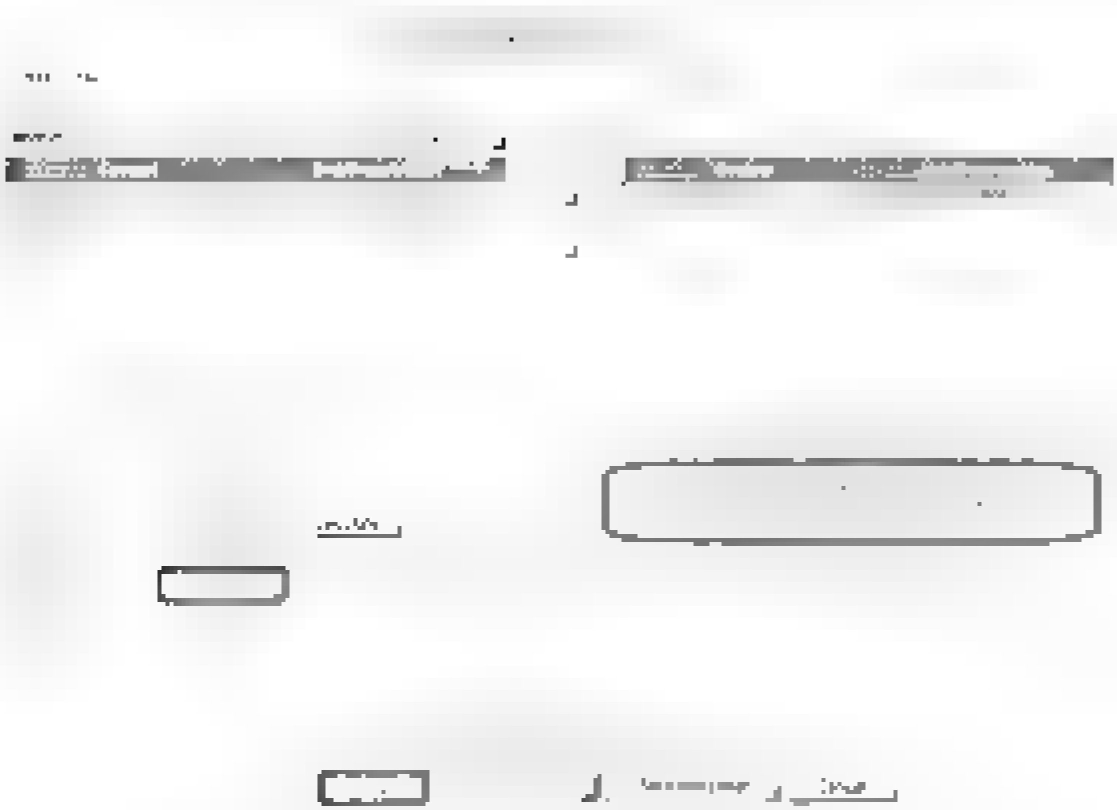
The Complaint Coordinator must also create an Investigator Package action in APCM. This is done by pressing the **Add Action**, **O-Complaints**, and select **Investigator Package**.



Once the Investigator Package Action Screen opens, search for the Complaint Coordinator's last name in the name field. Once found, select it and press > to bring it to the right hand side. The Date Created corresponds to the date the complaint was received by the CBSA. For the Due Date, enter the date provided by the Commissioner's Office. Next, enter your initials in the comments section. Once finished, press **Save**. This action will remain open until the information has been prepared and provided to the Commissioner's office via encrypted email or by regular post if the package is too large for email. If too large, a CD must be prepared by the Complaint Coordinator and mailed out. This information is to be recorded in the Investigator Package action's Comments section (this will reduce the number of mail-out actions created).



Once the Investigator Package is sent, this action must be closed. The Date Completed corresponds to the date that the information was sent. Add any pertinent details in the Comment section, as shown in the example below. Press Save when finished.



Most complaint correspondence emails are being received through the ATIP Generic Mailbox (Note to be changed to the ATIP Complaints Generic Mailbox). Once a Template Form request is received (Form A, Form B or EAW), the Complaint Coordinator creates the relevant action capturing the date received and the due date provided. The Date Completed action remains open until such a time as the approved template is returned signed to the OIC. If no date is provided by the OIC, the system will default to 14 days. The monitoring of these actions remains the responsibility of the Complaint Coordinator.

These template request actions are also found under **O-Complaints** tab in APCM

OIC_EAW

OIC_Form A

OIC_Form B

Once a template action has been created, the complaint file is ready to be assigned to an Analyst.

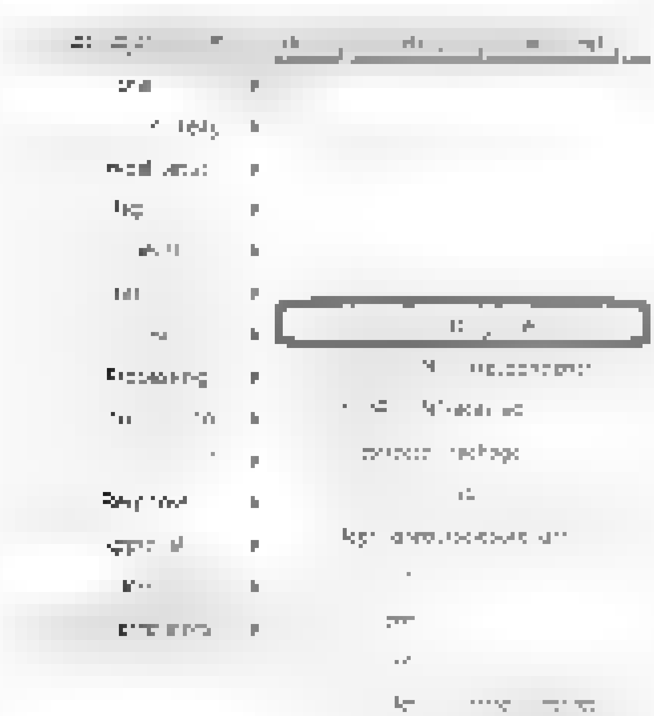
30.5 Assigning a Complaint

COMPLAINTassignment

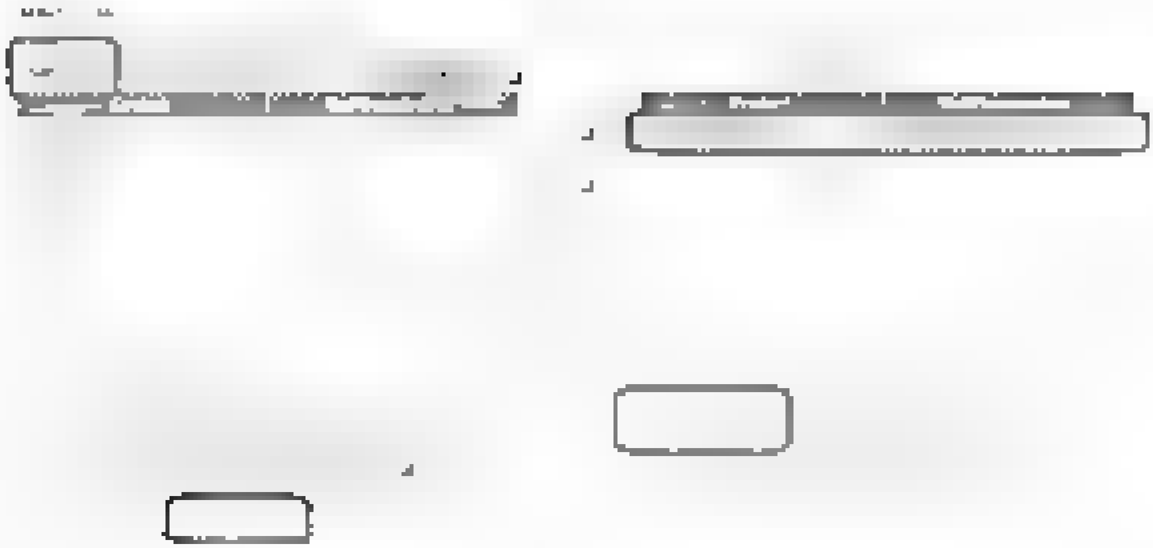
The **COMPLAINTassignment** action is used when more information is required by the Commissioner's Office to process the complaint, such as direct questions pertaining to how the file was processed. The action is also used when the OIC requests that a template (OIC EAW, OIC Form A and OIC Form B) be completed and returned to them.

This action is entered by selecting the **Add Action** tab, select **O-Complaints**, then **COMPLAINTassignment**.

Note: The action is to be entered by the Complaint Coordinator or the Assistant Director responsible for complaints.



This action is entered, in the same way as the AssignReview action. The Complaint Coordinator will search the last name of the chosen Analyst, select their name, and press the > to bring their name over to the right. The person creating the action should also add the text "Complaint assigned" and their initials in the Comment box as shown below.

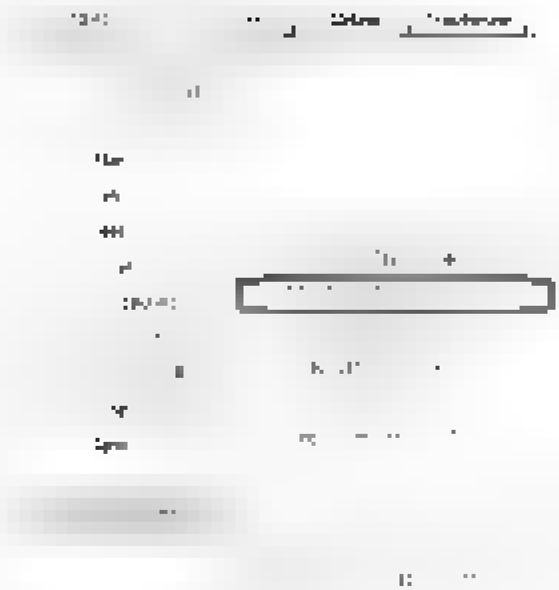


30.6 Processing a Complaint

COMPLAINTCorrespondence

COMPLAINTCorrespondence and its comment field are used to record and track the receipt of any correspondence between our office and the Commissioner. By selecting the action line and pressing **Email**, the Complaint Coordinator can send the Analyst an email to notify them that new correspondence has been received and scanned into Redaction for their review.

If the Analyst creates the action in APCM, these directives should be followed. Select the **Add Action** tab, then **O-Complaints** and selecting **COMPLAINTCorrespondence**. The Date Completed can be filled. The action will remain closed during the course of processing the file. However, the date closed should be amended each time a new item is received and entered into the Comment section of the **COMPLAINTCorrespondence** action.



LITIGATIONFlag

LITIGATIONFlag is used to record/flag, any litigation concerns on your complaint file

NegotiatedDisclosureDate

NegotiatedDisclosureDate is used to record if a specific disclosure date that has been determined/negotiated with the Commissioner. For this action, the Date Completed action will remain open until the required information has been successfully provided to the Commissioner. The monitoring of this action remains the responsibility of the Complaint Coordinator.

REPRESENTATIONSec35

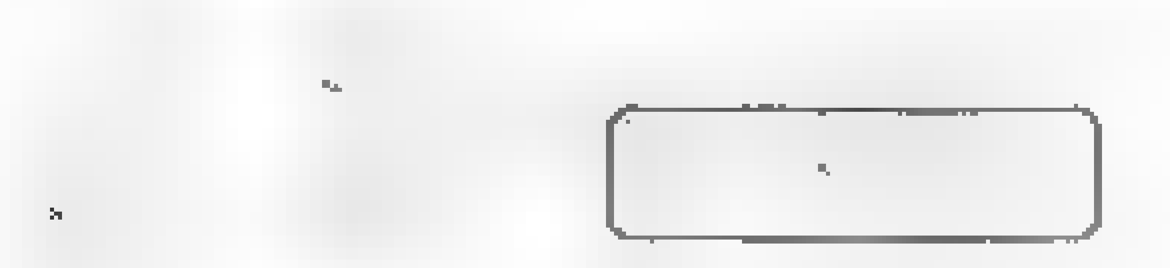
REPRESENTATIONSec35 is added to a file when the Commissioner asks us to provide further representations, in the course of a complaint investigation under the Act.

30.7 Closing a Complaint

Once all the information has been provided to the Commissioner, they will complete their review. When the Commissioner is satisfied with the information received, they will render their decision. This decision is provided to the CBSA via a document entitled "Record of Finding". This information must be entered in the APCM under the Complaints Tab to close the complaint (this information also needs to be imprinted to Redaction). Once the Record of Finding is received, the Complaint Coordinator may close the complaint.

To record this information, press the **Complaints** tab in APCM, and press **Edit**, selecting the correct complaint being addressed.

Here you will complete **Finding Date**, **Finding Result** and the **Date Closed** as it is specified in the Commissioner's findings letter. Once completed, press **Finish**.



Lastly, the **Complaint Coordinator** will need to select the **COMPLAINT received** action previously created in APCM, and populate the **Date Completed** date. This date is the date provided by the Commissioner on the "Record of Finding" document.

31 ACCESS TO INFORMATION ACT ARTICLES

Provision	Description	Category
10	Refusal to confirm or deny record exists	
13(1)(a)	Obtained in confidence from a government of a foreign state	Mandatory* Class *Subsection 13(2) does allow for disclosure if the originator consents to the disclosure or if they make the information public
13(1)(b)	Obtained in confidence from an international organization	
13(1)(c)	Obtained in confidence from a government of a province	
13(1)(d)	Obtained in confidence from a municipal or regional government	
13(1)(e)	Obtained in confidence from an aboriginal government	
14(a)	Federal-provincial affairs – consultations or deliberations	Discretionary Injury
14(b)	Federal-provincial affairs – strategy or tactics relating to the conduct of federal-provincial affairs	
15(1) Def	Defence of Canada	Discretionary Injury
15(1) IA	International relations	
15(1) SA	Prevention or suppression of subversive or hostile activities	
16(1)(a)(i)	Obtained or prepared by an investigative body in the course of a lawful investigation pertaining to the detection, prevention or suppression of a crime	Discretionary Injury
16(1)(a)(ii)	Obtained or prepared by an investigative body in the course of a lawful investigation pertaining to the enforcement of any law of Canada or a province.	
16(1)(a)(iii)	Obtained or prepared by an investigative body in the course of a lawful investigation pertaining to activities suspected of constituting threats to the security of Canada	
16(1)(b)	Investigation techniques or plans for specific lawful investigations.	
16(1)(c)	Injurious to the enforcement of any law of Canada or a province or the conduct of lawful investigations	
16(1)(d)	Injurious to the security of penal institutions	

16(2)	Security – Could facilitate the commission of an offence (other or when not wanting to specify)	
16(2)(a)	Security – Criminal methods or techniques	
16(2)(b)	Security – Technical information relating to weapons or potential weapons	
16(2)(c)	Security – Vulnerability of buildings structures, systems and methods to protect them	
16(3)	Obtained or prepared by RCMP while performing policing services for a province or municipality	Mandatory Class
16.5	Created for purpose of making a disclosure under the Public Servants Disclosure Protection Act or in the course of an investigation into such a disclosure	Mandatory Class
17	Safety of individuals	Discretionary Injury
18(a)	Trade secrets or financial, commercial, scientific or technical information belonging to the Government of Canada or a government institution and has substantial value.	Discretionary Class
18(b)	Could prejudice the competitive position of a government institution or to interfere with contractual or other negotiations of a government institution	
18(c)	Scientific or technical information obtained through research by an officer or employee of a government institution which could deprive the officer of priority of publication.	Discretionary Injury
18(d)	Materially injurious to the financial interests of the Government of Canada.	
18.1(1)(a)	Trade secret or financial, commercial, scientific or technical information that belongs to, and has consistently been treated as confidential by the Canada Post Corporation	
18.1(1)(b)	Trade secret or financial, commercial, scientific or technical information that belongs to, and has consistently been treated as confidential by the Export Development Canada	Discretionary* Class *Subsection 18.1(1) does not apply to the general administration of said institutions or any activity of Canada Post Corporation that
18.1(1)(c)	Trade secret or financial, commercial, scientific or technical information that	

	belongs to, and has consistently been treated as confidential by the Public Sector Pension Investment Board	is fully funded out of moneys appropriated by Parliament
18.1(1)(d)	Trade secret or financial, commercial, scientific or technical information that belongs to, and has consistently been treated as confidential by VIA Rail Canada Inc.	
19(1)	Personal information	**Mandatory* Class** * Information may be disclosed if individual consents, information is publicly available or in accordance with section 8 of the Privacy Act.
20(1)(a) 20(1)(b) 20(1)(b.1)	Trade secrets of a third party Financial, commercial, scientific or technical information that is confidential information supplied to a government institution Information supplied in confidence to a government institution by a third party for preparation, maintenance, testing or implementation by the government institution of emergency management plans and that concerns the vulnerability of the third party's buildings or other structures, its networks or systems	**Mandatory* Class** *Subsection 20(1) does not apply results of product or environmental testing. Information protected under paragraphs 20(1)(b) to (d) can be released with consent or in the public interest (public health, public safety or protection of the environment) and the public interest in disclosure clearly outweighs in importance any financial loss or gain to a third party or other injury.
20(1)(c) 20(1)(d)	Material financial loss or gain or prejudice to the competitive position of a third party. Interference with contractual or other negotiations of a third party	**Mandatory* Class** *Subsection 20(1) does not apply to results of product of environmental testing Information protected under paragraphs 20(1)(b) to (d) can be released with consent or if in the public interest (public health, public safety or protection of the environment) and the public

		interest in disclosure clearly outweighs in importance any financial loss or gain to a third party or other injury.
21(1)(a)	Advice or recommendations developed by or for a government institution or a minister of the Crown.	**Discretionary* Class** *Exemptions expire after 20 years
21(1)(b)	Consultations or deliberations in directors, officers or employees of the Crown or the staff of a minister participate	Does not apply to decisions made in the exercise of a discretionary power or an adjudicative function and that affects the rights of a person.
21(1)(c)	Positions or plans developed for the purpose of negotiations carried on or to be carried on by or on behalf of the Government of Canada	
21(1)(d)	Plans relating to the management of personnel or the administration of a government institution that have not yet been put into full operation	Does not apply to reports prepared by consultants or advisers who were not a director, an officer or an employee of a government institution or a member of the staff of a minister of the Crown
22	Testing or auditing procedures or techniques or details of specific test to be given or audits to be conducted	**Discretionary Injury**
22.1(1)	Draft report of an internal audit or any related audit working paper if the record came into existence less than fifteen years before the request was made	**Discretionary* Class** *Does not apply if a final report of the audit is not delivered to the institution within two years of commencement
23	Solicitor client privilege	**Discretionary Class**
24(1)	Information the disclosure of which is restricted by or pursuant to any provision set out in Schedule II of the Act	**Mandatory Class**
26	Material that will reasonably be published within ninety days of the request being made or within such further period of time as may be necessary for printing or translating the material for the purpose of printing it	**Discretionary Class**

Provision	Description	Does not include:
68(a)	Published material or material available for purchase by the public	
68(b)	Library or museum material preserved solely for public reference or exhibition purposes.	
68(c)	Material placed in the Library and Archives of Canada, national museums or on behalf of persons or organization other than government institutions	
69(1)(a)	Memoranda the purpose of which is to present proposals or recommendations to Council	
69(1)(b)	Discussion papers the purpose of which is to present background explanations, analyses of problems or policy options to Council for consideration by Council in making decisions	Confidences of the Queen's Privy Council for Canada that have been in existence for more than twenty years. OR
69(1)(c)	Agenda of Council or records recording deliberations or decisions of Council	Discussion papers described in paragraph (1)(b)
69(1)(d)	Communications or discussion between Ministers of the Crown on matters relating to the making of government decisions or the formulation of government policy	Decision has been made public. OR If the decision has not been made public, if four years have passed since the decision was made
69(1)(e)	Records the purpose of which is to brief ministers of the Crown in relation to matters that are before, or are proposed to be brought before, Council or that are the subject of communications or discussions referred to in paragraph (d)	
69(1)(f)	Draft legislation.	
69(1)(g)	Records that contain information about the contents of any record within a class of records referred to in paragraphs (a) to (f)	
69	Where a certificate under 38 of the Canada Evidence Act prohibiting the disclosure of information contained in a record	

32. PRIVACY ACT ARTICLES

Provision	Description	Category
3(j)	Not personal information	
18(1)	Exempt banks – s.21 international affairs and defence OR s.22 law enforcement and investigation	Discretionary Class
18(2)	Exempt banks – under subsection 12(1) right of access OR s.18(1)	
18(3)(a)	Exempt banks	
18(3)(b)	Exempt banks	
19(1)(a)	Personal information obtained in confidence from a foreign state or an institution thereof	Mandatory* Class
19(1)(b)	Personal information obtained in confidence from an international organization of states or an institution thereof	*Subsection 19(2) does allow for disclosure if the originator consents to the disclosure or if they make the information public.
19(1)(c)	Personal information obtained in confidence from a province or an institution thereof	
19(1)(d)	Personal information obtained in confidence from a municipal or regional government or an institution of such a government	
20	Federal-provincial affairs	Discretionary Injury
21	International affairs, defence of Canada or any state allied or associated with Canada, or efforts of Canada toward detecting, preventing or suppressing subversive or hostile activities	Discretionary Injury
22(1)(a)(i)	Obtained or prepared by an investigative body in the course of a lawful investigation pertaining to the detection, prevention or suppression of a crime	Discretionary** Class
22(1)(a)(ii)	Obtained or prepared by an investigative body in the course of a lawful investigation pertaining to the enforcement of any law of Canada or a province	**Subparagraphs 22(1)(a)(i) to (iii) do not apply if information came into existence 20 years prior to the request
22(1)(a)(iii)	Obtained or prepared by an investigative body in the course of a lawful investigation	

	pertaining to activities suspected of constituting threats to the security of Canada	
22(1)(b)	Law enforcement or conduct of lawful investigations	Discretionary Injury
22(1)(c)	Security of a penal institution	
22(2)	Obtained or prepared by the RCMP while performing policing services for a province or municipality	Mandatory Class
22.3	Created for the purpose of making a disclosure under the Public Servants Disclosure Protection Act or in the course of an investigation into such a disclosure	Mandatory Class
23(a)	Obtained or prepared by an investigative body for the purpose of determining whether to grant security clearances required by the Government of Canada or a government institution	Discretionary Class
23(b)	Obtained or prepared by an investigative body for the purpose of determining whether to grant security clearances required by the Government of a province or a foreign state or an institution thereof	
24(a)	Collected or obtained by CSC or NPB while the requester was under sentence for an offence if disclosure could lead to a serious disruption of their institutional, parole or statutory release programs	Discretionary Injury
24(b)	Collected or obtained by CSC or NPB while the requester was under sentence for an offence if disclosure could reveal information about the individual originally obtained on a promise of confidentiality	
25	Safety of an individual	Discretionary Injury
26	Personal information of another individual in accordance with Section 8	Mandatory Class
27	Solicitor-client privilege	Discretionary Class
28	Medical records	Discretionary Injury

Provision	Description	Does not include:
69(1)(a)	Library or museum material made or acquired and preserved solely for public reference or exhibition purposes.	
69(1)(b)	Material placed in NAC, NLC, NGC, CMC, CMN or the NMST by or on behalf of persons or organizations other than government institutions	
70(1)(a)	Memoranda the purpose of which is to present proposals or recommendations to Council	Confidences of the Queen's Privy Council for Canada that
70(1)(b)	Discussion papers the purpose of which is to present background explanations, analyses of problems or policy options to Council for consideration by Council in making decisions	have been in existence for more than twenty years; OR
70(1)(c)	Agenda of Council or records recording deliberations or decisions of Council.	Discussion papers described in paragraph (1)(b)
70(1)(d)	Communications or discussion between Ministers of the Crown on matters relating to the making of government decisions or the formulation of government policy	Decision has been made public, OR if the decision has not been made public, if four years have passed since the decision was made
70(1)(e)	Records the purpose of which is to brief ministers of the Crown in relation to matters that are before, or are proposed to be brought before, Council or that are the subject of communications or discussions referred to in paragraph (d)	
70(1)(f)	Draft legislation	
70	Where a certificate under s. 39 of the *Canada Evidence Act* prohibiting the disclosure of information contained in a record is issued before a complaint is filed under this Act	

33. CRIMINAL OFFENCE UNDER THE ACCESS TO INFORMATION ACT (s. 67.1)

In the absence of a specific request, records may be destroyed according to our retention periods and in accordance with the Retention and Disposal schedules set out by the National Archives.

However, even in the absence of a specific Access to Information Act (ATIA) request, anything done to intentionally "deny a right of access" under the ATIA can result in criminal prosecution (i.e. a decision making document is shredded because it may fall under the scope of a future request).

A suspected violation of section 67.1 of the ATIA is treated in a similar fashion to a suspected theft, destruction of property or other security breach which may involve criminal activity.

67.1 (1) No person shall, with intent to deny a right of access under this Act,
(a) destroy, mutilate or alter a record;
(b) falsify a record or make a false record;
(c) conceal a record; or
(d) direct, propose, counsel or cause any person in any manner to do anything mentioned in the any of paragraphs (a) to (c).

(2) Every person who contravenes subsection (1) is guilty of
(a) an indictable offence and liable to imprisonment for a term not exceeding two years or to a fine not exceeding $10,000, or to both; or
(b) an offence punishable on summary conviction and liable to imprisonment for a term not exceeding six months or to a fine not exceeding $5,000, or to both

34. PROGRAMS AND INFORMATION HOLDINGS (FORMERLY INFO SOURCE)

All government institutions subject to the Access to Information Act and the Privacy Act publish an inventory of their information holdings as well as relevant details about personal information under their control.

You can browse the list of government institutions to learn more about their programs, activities, and information holdings, including their classes of records and personal information banks (PIBs).

Some programs and activities are common to most government institutions. They are known as internal services and they involve the following types of information:

- Standard classes of records: These are descriptions of all records created and used to support internal services.
- Standard personal information banks: These are descriptions of personal information contained in records and collected and used to support internal services.

More information on Canada Border Services Agency's institutional functions, programs and activities including the different classes of Records and Personal Information Banks can be found here:
https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/infosource-eng.html

34.1 Informal Requests

When a True Access request of information has been done previously, an Analyst can offer the requester the information through an informal process. This is attractive to many, as they will get the information they are seeking more quickly.

Completed Access to information (ATI) summaries can be founds here:

https://open.canada.ca/en/search/ati?f%5B0%5D=ss_ati_organization_en%3ACanada%20Border%20Services%20Agency

To obtain information informally, the requester can submit their request as they would any other Access to Information or Privacy Act request.

ANNEX A. OPERATIONS TEAM CHECKLIST

Receiving and Opening New Requests

<u>Edit Screen</u>

- ✓ **Request Type** – verify for accuracy
- **Requester** – verify it accurate/complete, including prefix and address. Ensure it's not a duplicate.
- **Source** – verify for accuracy.
- **Requester's File Number** – should be added if applicable
- ✓ **Date Complete Received** – day request was received by the CBSA office
- ✓ **Full Text – Summary** – Spell check (F7), all details are accurate/complete with no spelling mistakes.
- **Request Transferred In** – "Checked" if request transferred from another institution
- **Preferred Method of Access** – Select only if indicated by Requester
- **Translation Requested** – Select only if indicated by Requester

<u>Records</u>

- Check that all documents are in Redaction (initial correspondence, payment, supporting docs)
- Records above Protected B must not be scanned into Redaction

<u>Activity Screen</u>

- **Initial/SetUp** – opened and closed – ensure it follows our standardized model
  - online – (your initial)
  - fax – (your initial)
  - email – (your initial)
  - paper – (your initial)
- **Cross-Reference** (as appropriate) – opened and closed – indicate the cross referenced file; the file cross referenced should also have a ref action added.
- ✓ **Payment Attached** (as appropriate) – opened and closed – should contain payment info: Cheque # – Cash/Receipt # (online requests), and Amount.

<u>Fee Screen</u>

- ✓ Fees and payments should only be entered
- Application Fee – date complete received – $5.00
- Payment Received fee type (do not add if no payment was received)
- ✓ If the request is transferred from another institution (and the $5.00 fee received by them) add in the comments "Application fee $5.00, request was transferred from other institution"

Closing the File

<u>Activity Screen</u>

- All actions must be closed (with appropriate dates). Contact the Analyst if this is not complete
- Ensure Moved Out action is present. Contact the Analyst if this is not complete

<u>Fee Screen</u>

- No outstanding fees, unless the file is abandoned. Contact the Analyst if this is not complete.

<u>Closing Screen</u>

- Closing Screen must be accurate and complete. Contact the Analyst if this is not complete

- **Date Closed and Decision** – automatically filled in by the Operations Team when file is closed, unless the file is abandoned in which case the Analyst completes both fields.

ANNEX B ANALYST AND TEAM LEADER CHECKLIST

Receiving New Requests

Edit Screen

- **Request Type** – verify for accuracy.
- **Category** – verify and change if needed.
- **Requester** – verify if accurate/complete, including prefix and address. Ensure it's not a duplicate.
- **Source** – verify for accuracy.
- **Requester's File Number** – should be added if applicable.
- **Decision Maker** – verify correct name.
- **Date Complete Received** – day request was received by the CBSA office, or day request was received by transferring department (Access requests only).
- **Full Text** – **Summary** – spell check (F7), all details are accurate/complete with no spelling mistakes.
- **Request Transferred In** – "Checked" if request transferred from another institution.
- **Preferred Method of Access** – Select only if indicated by Requester.
- **Translation Requested** – Select only if indicated by Requester.

Records

- Check that all documents are in Redaction (initial correspondence, payment, supporting docs) indexed and stacked.
- Records above Protected B must not be scanned into Redaction.

Activity Screen

- *Initial/Set-Up* – opened and closed.
- *Cross Reference* (as appropriate) – opened and closed.
- *Payment Received* (Access requests only, as appropriate) – opened and closed.
- *Assign/Review* action – added by the TL assigning the file indicating who was assigned the file opened and closed.

Fee Screen

- Fees and payments should only be entered for Access Requests.
- Application Fee (code 1) amount received: $5.00 (note that an application fee is not refundable).
- Payment Received fee type (do not add if no payment was received).
- If the request is transferred from another institution (and the $5.00 fee received by them) add in the comments "Application fee $0.00, request was transferred from other institution".

Processing the File

Incomplete / On Hold

- Use **Action Incomplete** to put the request on hold when more information is needed, or a fee hasn't been received (if an Access request). Indicate in the comments section as to the reason the file is being placed on hold.
- If you call, use the appropriate action, but after three days generate the appropriate letter. Do not abandon without having sent a letter or email offering the requester 30 days to respond.
- If request is on hold, close all open retrieval actions and notify OPIs that the request is being clarified and that you will advise them when clarification is received or if request is abandoned.

Extension Screen

- Ensure you add ALL relevant **EXTEND** actions in APCM to indicate the reasons for the extension.
- Make sure you enter the amount of time taken for all extensions (if you take 30 days, do not set one to 30 and the other to zero) using your EXTENSION button.
- Do NOT take extension if request has not yet been completely received (on hold for clarification, fees, etc.)
- ✓ You MUST take extensions within first 30 days of completely received request.

Retrieval Notice

- Use the **RETRIEVAL notice** action for tasking to the program area for responsive records.
- ✓ Close retrieval actions when the request is on hold; add new retrieval actions once the request is no longer on hold.
- Close retrieval actions when records or response and routing slip / recommendations memo is received.
- Use **CONSULT-Int** when consulting OPIs internally for disclosure recommendations on records.

SECRET, Protected C / Confidential or above

- ✓ Records above Protected B classification must NOT be scanned into Redaction (security incident). Image (or above Protected B) must be SECRET scanning / printing to Redaction. Records should be processed using the standalone computer (up to SECRET level) and the severed version of the records are to be scanned into Redaction afterwards.
- ✓ For records classified TOP SECRET or higher, speak to your Team Leader and Assistant Director for advice on how to proceed.
- Exemptions should be applied or be manually added in the EXEMPTIONS screen in APCM.
- ✓ Add the **DOCType (A)** action to record the type of records on file.

Ready for Approval

- Double check the category is accurate in EDIT screen.
- ✓ Ensure that the Decision Maker is the person that will be signing the response letter (before creating your letter).
- Add the proper **APPROVAL** action with the name of the approver as the contact.

Once Approved (If True Access)

- Save the Release package to ATIP Briefing Folder (ensure if any changes were made, that it is the latest version).
- ✓ Check for flags – both formal and informal – and make sure all have been completed.
- Ensure the records have been uploaded to the *Public Safety Portal*.

Closing the File

Edit Screen

- ✓ **Request Type** – verify for accuracy.
- **Category** – verify for accuracy.
- **Requester** – verify if accurate/complete, including prefix and address.
- ✓ **Source** – verify for accuracy.
- **Decision Maker** – verify for accuracy.
- **Pages Received** – verify for accuracy.
- **Preferred Method of Access** – verified if completed and followed.

Records

[illegible] that all document[illegible] [illegible] Redaction [illegible] [illegible] payment [illegible] [illegible]

[illegible] must [illegible] be [illegible] into Redaction [illegible] the [illegible]

[illegible]

Activity Screen

All [illegible] may be [illegible] before the file [illegible] dates [illegible]

Closed [illegible] opened and closed [illegible] for all [illegible] requests

[illegible]

[illegible] and password protected [illegible] information

[illegible] **COMPLEXITY** [illegible] during the request [illegible]

[illegible]

Fee Screen

There should be no outstanding fees unless the file [illegible] abandoned [illegible] of payment for the application fee

Exemptions Screen

[illegible] should be [illegible]

Closing Screen

[illegible] package [illegible]

[illegible] pages [illegible] released and pages not released [illegible] pages [illegible] reviewed

The closing [illegible] must be accurate and complete

- **Disposition** – [illegible] package [illegible]
  Method of Access, **Delivery** and **Translation** must be complete
  Request Transferred On [illegible]
  Translation Requested [illegible] requested [illegible]
  Comments [illegible]
- **Reason for Deemed Refusal** [illegible] appropriate reason [illegible] the delay
- **Manual Pages** – ensure that you indicate manual pages reviewed, released and not released [illegible] manual pages [illegible] Redaction [illegible] will have to [illegible]

The [illegible] will [illegible] the **Date Closed** and **Decision Communicated** [illegible] both fields

ANNEX C. ATIP IMMIGRATION TASKING GRID

Requested Records	OPIs to Task
Complete immigration file or ou Copie complète dossier d'immigration	Programs OPS Region FOSS GCMS
In Canada file or ou Dossier au Canada	Programs OPS Region FOSS GCMS
All records/docs held by CBSA ou Copie complète de tous les documents que détient l'ASFC	Programs OPS Region FOSS GCMS Full ICES Exit Report
Client file or ou Dossier client	Programs OPS Region FOSS GCMS
All records held in a specific location/region or ou Copie complète de tous les documents à un endroit/région précis	Region FOSS GCMS
Complete immigration file including visa/overseas file or ou Copie complète dossier d'immigration incluant le dossier visa/outremer	Programs OPS Region FOSS GCMS
In Canada in a specific location/region or ou Dossier au Canada à un endroit/région spécifique	Region FOSS GCMS

ANNEX D: STACKING AND INDEXING

LEGEND TO ATIP STACKS

Stack Alias	Stack Name
ADMIN	Administrative File
PD-VPO	Vice-President Office
OPS	Operations Branch
PROG	Programs Branch
HQ-HR	Human Resources Branch – HQ
COMP	Comptrollership Branch
ISTB	Information, Science & Technology Branch
SPB	Strategic Policy Branch
ATL	Atlantic Region
PAC	Pacific Region
PRA	Prairie Region
PRA-HR	Prairie Region HR
GTA	Greater Toronto Area
SOR	Southern Ontario Region
SOR-HR	Southern Ontario Region HR
NOR	Northern Ontario Region
QUE	Quebec Region
REC	Records for Processing
FOSS	FOSS Print out
GCMS	GCMS Print out
EDOC	GCMS eDocs

ICES	Travel History
EXITS	Exit Reports
VETTED	Records to be Vetted
SPSD	Security & Professional Standards Directorate
LEGAL	Legal Services Unit (CBSA)
OIC	Office of the Information Commissioner
OPC	Office of the Privacy Commissioner

LEGEND TO ATIP INDEX SUBJECTS

Common Admin Record Index Subject Lines

Text Entered	Used:
Original Request	Request
Payment	For ATIA requests only
Consent	Valid consent
X Consent	Invalid consent
Ack incomplete	Any written acknowledgement incomplete letters & emails
Retrieval Notice	Outgoing email from ATIP to OPI
Nil – Retrieval	Incoming email from OPI to ATIP with no records response
Retrieval Response	Incoming email from OPI to ATIP indicating records exist
Routing	Signed Routing Slip with record and Concerns indicated
Routing – NO	Signed Routing Slip and No Objections/Concerns
Nil – Routing	Routing slip from OPI with no records response
Recommendations	The disclosure recommendation memo received from OPIs for use with all files (e.g. regular files, consultations, vettings, etc.)
Consult – NO	Incoming memo or email from OPI to ATIP with No Objections/Concerns to disclosure
Consult	Incoming memo or email from OPI to ATIP with Identified Objections/Concerns to disclosure

Response	Response letter to requesting party with the redacted records. Applies to all paper response letters for all files (e.g., regular files, consultations, vettings, etc.).

ANNEX E LETTER INSERTS

ACK/INCOMPLETE LETTERS

request through an individual who has right of access

passport, valid visa, citizenship card). You may resubmit your request under the Access to Information Act, along with an application fee of $5.00.

- Requests made under the Privacy Act require that you be a Canadian citizen, a permanent resident or an individual presently in Canada. Please provide proof that you are entitled to make a request under the Privacy Act (i.e., copy of a stamped passport, valid visa, citizenship card). You may resubmit your request under the Access to Information Act, along with an application fee of $5.00, through an individual who has right of access. Your written consent authorizing him/her to receive your personal information is required.

PAYMENT

- Note that an application fee of $5.00 is required (cheque or money order made payable to the Receiver General of Canada) to process an Access to Information request.

- Please be advised that you are entitled to submit your request under the Privacy Act. In order to do so, we require your written confirmation, either by facsimile or letter. If you have not already done so, please submit proof that you are entitled to make a request under the Privacy Act (i.e. either one of the following: stamped passport, valid visa, permanent resident card, and the Canadian citizenship card).

- We are returning your $5 cheque/money order as there are no fees under the Privacy Act (ONLY use for cash or cheque payments).

- The request you submitted only requires a $5.00 application fee. Therefore, I am returning your $$$ cheque / money order. Please re-submit a $5.00 cheque / money order.

- The requests you submitted will be processed as one. I am therefore returning your $$ cheque / money order. Please re-submit a $5.00 cheque / money order.

- The cheque / money order you provided was not made out to the Receiver General of Canada. Please resubmit another cheque.

- The cheque / money order you provided was not signed. Please sign and return your cheque / money order.

CONSENT

- The consent of name of applicant(s) is required to process your request. To be valid, a consent must be signed, dated, and indicate to whom authority is given with the printed name of the person giving consent.

- A new consent from name of applicant(s) is required to process your request. To be valid, a consent must be signed, dated, and indicate to whom authority is given with the printed

name of the person giving consent. The consent provided does not indicate your client's name.

- A new consent from name of applicant(s) is required to process your request. To be valid, a consent must be signed, dated, and indicate to whom authority is given with the printed name of the person giving consent. The consent provided was not dated.

- A new consent from name of applicant(s) is required to process your request. To be valid, a consent must be signed, dated, and indicate to whom authority is given with the printed name of the person giving consent. The consent provided was not signed.

- A new consent for name(s) of the applicant(s) is required to process your request, as information was added after it was signed.

- A new consent for name(s) of the applicant(s) is required to process your request, as the date was added after it was signed.

- A new consent, <u>that includes to whom authority is given</u>, for name is required. To be valid, a consent must be signed, dated, and indicate to whom authority is given with the printed name of the person giving consent.

- A new, recent consent is required. A valid consent form can be found here: <u>http://www.cbsa-asfc.gc.ca/publications/forms-formulaires/bsf745-eng.html</u>

- If you have not already done so, when submitting an Access or Privacy request, we recommend you provide a "consent to disclose personal information" statement, signed and dated by each adult individual (over 18 years old) contained in the client file that you are accessing. Providing consent from all parties with your Access request enables CBSA to release information relating to these third parties in conformity with the Privacy Act.

- The consent you have provided does not authorize Canada Border Services Agency to release information to you. A valid consent form can be found here: http://www.cbsa-asfc.gc.ca/publications/forms-formulaires/bsf745-eng.html

- The consent you have provided does not give you authority to obtain all the information you have requested. Please either amend your request or provide a new consent authorizing you to obtain what you have requested.

- Customs consent is required in order to process your request. To be valid, a consent must be signed, dated, and indicate to whom authority is given with the printed name of the person giving consent. As well, consent should be on company letterhead and be an authorized representation of that company, such as a President or CEO.

- Pursuant to the *Privacy Act*, if a person has been dead for less than 20 years, only the executor of the estate or one having Power of Attorney may request the deceased's personal

information to administer the estate of that person, but <u>only for the purpose of such administration. Please provide the purpose of request, proof of death and proof of executorship or court order (copy).</u>

- The *Privacy Act* or the *Access to Information Act* requires that a third party provide one of the following: consent, proof that the person has been dead for more than 20 years (i.e. copy of obituary notice, death certificate, photos of tombstones, Provincial Vital Statistics) or proof that a person has been appointed, pursuant to the laws of Canada, to administer the estate but only for the purpose of such administration (i.e. letter of administration from the court, copy of the will).

- Unless a person was born over 110 years ago, reasonable proof of death is required (Section 3(m) of the *Privacy Act* states that personal information can be released if an individual has been deceased for more than twenty years) i.e. copy of obituary notice, death certificate, photos of tombstones, Provincial Vital Statistics.

- Note: the information requested cannot be released as the person died less than 20 years ago. Section 3(m) of the *Privacy Act* states that personal information can be released if an individual has been deceased for more than twenty years.

- Pursuant to the *Privacy Act* if a person has been dead for less than 20 years, only the executor of the estate or one having Power of Attorney may request the deceased's personal information to administer the estate of that person, but only for the purpose of such administration.

MISSING INFORMATION

- Your client's FULL name
- Your client's date of birth
- Your client's Client ID
- Your client ID
- Your date of birth

MISCELLANEOUS

- Note: Under the *Access to Information Act* or the *Privacy Act*, the Canada Border Services Agency Access to Information and Privacy Division does not respond to questions but only provides copies of existing records.

NO RECORDS LETTERS

- The processing of your request is now complete. The information you have requested is publicly available. Section 68 of the Act excludes from the disclosure of published material or

material available for purchase by the public. However, we are providing a website, where the information can be obtained: http://publications.gc.ca/

- The processing of your request is now complete. After a thorough search, no records were found that respond to your request. However, there is indication that records may be held by Immigration, Refugees and Citizenship Canada. You may submit a request to Immigration, Refugees and Citizenship Canada

at the following address:

Immigration, Refugees and Citizenship Canada
Audrey White
A/Access to Information and Privacy Coordinator
Narono Building
360 Laurier Avenue West, 10th Floor
Ottawa, Ontario K1A
Telephone: 1-800-667-6703
Other Telephone: 1-800-667-6703
Facsimile: 613-957-6517
ATIP-AIPRP@cic.gc.ca
ATIP Online Request

(Check to ensure this is still the correct coordinator at http://www.tbs-sct.gc.ca/hgw-cgf/oversight-surveillance/atip-aiprp/coord-eng.asp)

LATE RESPONSE PARAGRAPH

The Canada Border Services Agency is experiencing record high volumes of *Access to Information Act* (or *Privacy Act*) requests. The Agency remains committed to ensuring that every reasonable effort is made to respond to all requests as soon as possible. Your request will be completed by [illegible], 2019. We apologize for the delay in responding and any inconvenience this may have caused.

If we cannot commit to a completion date do not include one

ANNEX F: TIPS AND TRICKS

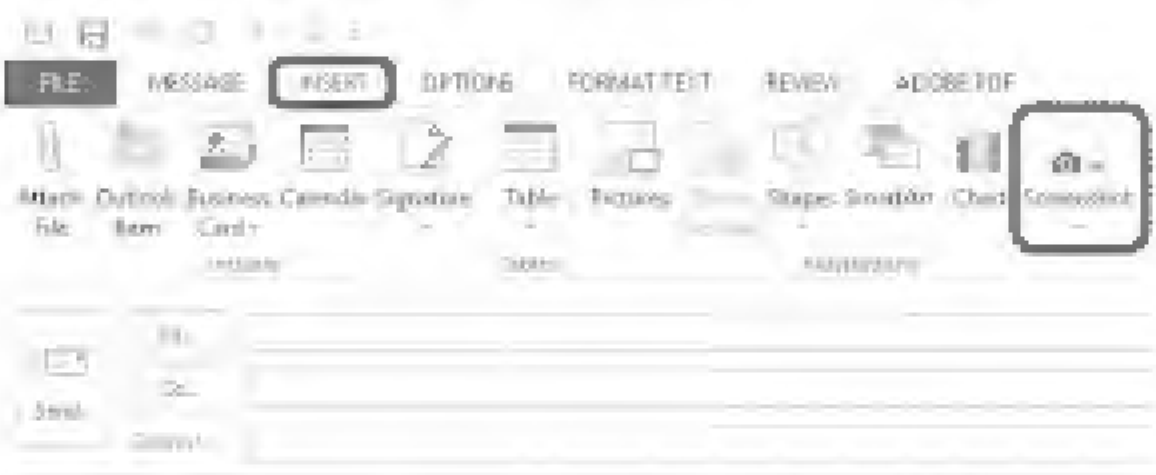
<u>**How to put a Screen Shot in an Email**</u>

<u>Note</u>: *When you are sending screen captures via email, please ensure the email is always encrypted as per security policy.*

There are several different ways to provide screenshots to people seeking them.

1. If someone is asking you to email a screenshot do the following:

   Open a new message in Outlook, and go to the Insert tab and select the Screenshot icon:



   When you open the Screenshot function, you will get the option of either adding an entire window that is open on your computer, or adding a Screen Clipping.

The Screen Clipping option allows you to highlight a specific section on your computer screen. When you select Screen Clipping, your screen will go translucent white and crosshairs will appear on your screen. Hold your left mouse button and drag the cursor to produce a window. Anything in that window will be captured. When you let go of the mouse button, the image that you captured will appear in your email.

Picking any of the Available Windows seen in the screenshot option will automatically add the image shown to your email.

2. Alternatively, you can use windows shortcut keys.

Print Scrn = will capture everything on the screen. If you have two monitors, this means the image produced will include both screens.

Alt + Print Scrn = will capture only the screen you have active.

The same procedures can be done in Word.

ANNEX G: RETENTION OF FORMS

When an ATIP request comes in for a certain form, you can use this chart to look up its retention period.

ANNEX H: INFORMATION CLASSIFICATION GUIDE

Canada Border Services Agency's Information Classification Guide is a valuable tool to determine the Security level of any records.